OfficeServ 7200

Data Server User Manual

Every effort has been made to eliminate errors and ambiguities in the information contained in this booklet. Any questions concerning information presented here should be directed to SAMSUNG TELECOMMUNICATIONS AMERICA. SAMSUNG TELECOMMUNICATIONS AMERICA disclaims all liabilities for damages arising from erroneous interpretation or use of information presented in this manual.

PUBLICATION INFORMATION

SAMSUNG TELECOMMUNICATIONS AMERICA reserves the right without prior notice to revise information in this publication for any reason.

SAMSUNG TELECOMMUNICATIONS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

COPYRIGHT 2005

Samsung Telecommunications America

All rights reserved. No part of this manual may be reproduced in any form or by any means—graphic, electronic or mechanical, including recording, taping, photocopying or information retrieval systems—without express written permission of the publisher of this material.

TRADEMARKS

Enterprise IP Solutions
OfficeServ™ is the registered trademark of SAMSUNG Electronics Co., Ltd.
Product names mentioned in this document may be trademarks and/or registered trademarks of their respective companies.

INTRODUCTION

Purpose

This document introduces the OfficeServ 7200 Data Server, an application of OfficeServ 7200, and describes procedures on installing and using the software.

Document Content and Organization

This document contains 3 chapters 3 annexes and an abbreviation as follows:

Chapter 1. OfficeServ 7200 Data Server Overview

This chapter briefly introduces the OfficeServ 7200 Data Server.

Chapter 2. OfficeServ 7200 Data Server Installation

This chapter describes the installation procedure and login procedure.

Chapter 3. Using the OfficeServ 7200 Data Server

This chapter describes how to use the menus of the OfficeServ 7200 Data Server.

Annex A. VPN Setting in Windows XP/2000

This chapter describes how to set VPN on Windows XP/2000.

Annex B. OfficeServ 7200 Data Server Quick Setup Guide

This Quick Setup Guide is designed to provide you with basic setup procedures of configuring your OfficeServ 7200 Data Server WAN1 port connecting to a DLS, Cable Modem or T1 for office wide Internet access sharing.

Annex C. OfficeServ 7200 Data Server Software Upgrade Quick Setup Guide

This Quick Setup Guide is designed to provide you with basic setup procedures of upgrading your OfficeServ 7200 Data Server software.

ABBREVIATION

Acronyms frequently used in this document are described.

© SAMSUNG Telecommunications America, L.P.

Conventions

The following special paragraphs are used in this document to point out information that must be read. This information may be set-off from the surrounding text, but is always preceded by a bold title in capital letters.

WARNING

Provides information or instructions that the reader should follow in order to avoid personal injury or fatality.

CAUTION

Provides information or instructions that the reader should follow in order to avoid a service failure or damage to the system.

CHECKPOINT

Provides the operator with checkpoints for stable system operation.

NOTE

Indicates additional information as a reference.

Console Screen Output

- The lined box with `'Courier New'` font will be used to distinguish between the main content and console output screen text.
- `'Bold Courier New'` font will indicate the value entered by the operator on the console screen.

© SAMSUNG Telecommunications America, L.P.

References

OfficeServ 7200 General Description Guide

The OfficeServ 7200 General Description Guide introduces the OfficeServ 7200 and provides system information including the hardware configuration, specification, and function.

OfficeServ 7200 Installation Guide

The OfficeServ 7200 Installation Guide describes the condition required for installation, the procedure of installation, and procedures on inspecting and starting the system.

OfficeServ 7200 Programming Manual

The OfficeServ 7200 Call Server Programming Manual describes the method of using the Man Machine Communication (MMC) program that changes system settings by using phones.

Revision History

Edition No.	Date of Issue	Remarks
01	09.2005	First Version

© SAMSUNG Telecommunications America, L.P.

SAFETY CONCERNS

For product safety and correct operation, the following information must be given to the operator/user and shall be read before the installation and operation.

Symbols

Caution

Indication of a general caution

Restriction

Indication for prohibiting an action for a product

Instruction

Indication for commanding a specifically required action

© SAMSUNG Telecommunications America, L.P.

CAUTION

Security Warning

Note that all external users are allowed to access the firewall when the Remote IP is set to '0.0.0.0' and Port is set to '0:'.

Setting IP Range

The number of IPs for the 'Local IP range' and that for the 'Remote IP range' should be identical.
For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

PPTP Setting in Windows XP/2000

In Windows XP/2000, the user can use DHCP client. If VPN PPTP client is connected while the DHCP client is operating, errors will be found. To prevent this problem, close the DHCP client operation on the [Start] → [Program] → [Administrative Tools] → [Services] menu of the Windows PPTP client installed.

Caution Against Changing Network Interfaces

If a network interface(e.g., IP, gateway, and subnet mask) is changed during router operation, all the IP sessions that are being used in the router are disconnected for a while.

DB Change

The DBs of the WIM module and LIM module are integrated in the OfficeServ 7200 Data Server. When the DB is changed, the system restarts.

Dynamic IP of DHCP, PPPoE, and xDSL

If a dynamic IP is used, information(e.g., 'Port Forward' and 'Static NAPT') on public IPs will not be automatically changed. **'Fixed IP' should be used for VoIP services that require settings of the 'Port Forward' and 'Static NAPT' menus and for VPN services that require WAN IP address setting.**

© SAMSUNG Telecommunications America, L.P.

Using Web Browser

Use Microsoft Internet Explorer 6.0 or higher as a Web browser to maintain OfficeServ 7200 Data Server.

Delete Temporary Internet Files

Delete Temporary Internet Files after upgrading Data Server package. After selecting the [Internet Explorer] → [Tools] → [Internet Options] menu, click the [Delete Cookies] and the [Delete Files] button in the [Temporary Internet files]. If Temporary Internet Files are not deleted, Data Server Web Management will not display properly.

© SAMSUNG Telecommunications America, L.P.

TABLE OF CONTENTS

INTRODUCTION 3

Purpose 3

Document Content and Organization 3

Conventions 4

Console Screen Output 4

References 5

Revision History 5

SAFETY CONCERNS 6

Symbols 6

War 7

TABLE OF CONTENTS 9

CHAPTER 1. OfficeServ 7200 Data Server Overview 12

OfficeServ 7200 Introduction 12

OfficeServ 7200 Data Server Introduction 13

CHAPTER 2. OfficeServ 7200 Data Server Installation 16

Installation Procedure 16

Configuring the PCs 17

Starting up the OfficeServ 7200 Data Server 19

CHAPTER 3. Using the OfficeServ 7200 Data Server 21

Firewall/Network Menu 22

Status 24

Management 27

Filtering Service 50

LAN Config 52

Switch Menus 53

Port 54

VLAN 57

MAC 62

© SAMSUNG Telecommunications America, L.P.

STP 64
IGMP Config 66
QoS Config 67
MISC Config 68
Save Config 69
Router Menus 70
General 70
Config 72
QoS Menus 77
Group 78
Policy 83
Status 84
Management 84
Status Menus 85
Monitoring 86
Statistics 88
Serial State 89
Services 90
VPN Menu 92
IPSec 93
PPTP 100
IDS Menu 103
Log Analysis 104
Configuration 109
Management 111
Rule Update 112
Block Config 113
Mail Config 115
DSMI Menu 116
DSMI Configuration 118
DHCP Server 122
VoIP NAPT 128

© SAMSUNG Telecommunications America, L.P.

SIP ALG Menu 129

Config 129

Management 131

System Menu 132

DB Config 133

Log 136

Time Config 138

Upgrade 141

Appl Server 143

Reboot 147

Home, My Info & Logout 148

ANNEX A. VPN Setting in Windows XP/2000 149

IPSec Setting 149

PPTP Setting 161

ANNEX B. OfficeServ 7200 Data Server Quick Setup Guide

ANNEX C. OfficeServ 7200 Data Server Software Upgrade Quick Setup Guide

ABBREVIATION

© SAMSUNG Telecommunications America, L.P.

CHAPTER 1. OfficeServ 7200 Data Server Overview

This chapter provides an overview of OfficeServ 7200 system and OfficeServ 7200 Data Server.

OfficeServ 7200 Introduction

The OfficeServ 7200 is a single platform that delivers the convergence of voice, data, wired, and wireless communications for small and medium offices. The 'office in a box' solution offers TDM voice processing, voice over IP integration, wireless communications, voice mail, computer telephony integration, data router and switching functions, all in one powerful platform.

With the LIM and WIM modules, the OfficeServ 7200 provides network functions such as a switch, router, and network security over the data server. This document describes the full suite of IP based data and routing capabilities of OfficeServ 7200 Data Server.

OfficeServ 7200 Configuration

For information on the configuration, features, or specifications of the OfficeServ 7200, refer to 'OfficeServ 7200 General Description Guide'.

OfficeServ 7200 Data Server Introduction

The OfficeServ 7200 provides the functions below on the IP-based data server:

Unmanaged Switch

- The switch performs the function of a layer 2 Internet switch as well as the Learning Bridge function based on the MAC address filtering and forwarding algorithm.
- The LIM module provides 16 LAN ports per module. Each port is 10/100 Base T, auto sending, full duplex. OS 7200 can support up to 8 unmanaged LIM.

Managed Switch

When the LIM is installed in slot 2 with a WIM in slot 1, it can function as a managed switch by using an access interface LAN on the WIM. OfficeServ 7200 supports 1 managed LIM.

As a managed switch, the following features are supported:

- 802.1D Spanning Tree – The switch configures and processes the forwarding tree based on the spanning tree algorithm to prevent a packet forwarding loop in the switch.
- Layer 2 802.1p Packet Priority QoS – The switch extracts the priority field from the Ethernet frame configured according to the 802.1p specification standard, and discriminatively processes the frame according to the priority of the specified operation. The switch then maps packets to a designated queue. Up to 2 output queues, Low and High, are supported per egress port with queuing type of Weighted Round Robin or All High before Low. For devices that do not support 802.1p, OS 7200 LIM can be configured to create an enforceable priority.
- Supports Virtual LAN (VLAN) – The Virtual Local Area Network (VLAN) groups the related equipment by the work group according to the LAN operational policy regardless of the location of the user equipment. VLAN removes the effects of unnecessary broadcasting packets and configures a stable switching subnet only for the corresponding group by separating and processing the group in the virtual LAN. The VLAN can be configured based on the switch port, MAC address, and 802.1Q tag.
- IGMP Snooping – IGMP Snooping provides a method for intelligent forwarding of multicast packets within a layer 2 broadcast domains. By snooping IGMP registration information, a distribution list of work stations is formed that determines which end-stations will receive packets with a specific multicast address.
- 802.3x Layer 2 Flow Control – Flow control is performed according to the value set for incoming rate and/or outgoing rate. Limiting the rate at which a port can receive or send traffic is used to ease congestion on bottlenecks in the network and provide simple prioritization when the network is busy.

© SAMSUNG Telecommunications America, L.P.

Router

- Multiple Network Interfaces:
  - 2 WAN Ethernet ports: auto-sensing 10/100Base-T and 10Base-T, supporting Point-to-Point, Point-to-Point over Ethernet (PPPoE) and DHCP client protocols.
  - 1 LAN Ethernet port: Enables a connection with a switch for LAN configuration.
  - 1 Serial WAN port: Enables dedicated data line service by being connected with DSU or CSU, which is a data line device. V.35 serial interface supports Dynamic Host Configuration Protocol (DHCP), PPP, or Frame Relay Encapsulation.
  - 1 DMZ Ethernet port: Enable DMZ connection to protect an internal network from external hazards. DMZ is a separate LAN port for configuring the device which requires a free access from outside such as a mail server and web server, while separating the device from internal devices.
- Subnet Routing – The network interfaces of the WAN1, WAN2, LAN and DMZ are configured with different sub-network interfaces, which enable them to perform the routing process with each other.
- Static Routing – The OfficeServ 7200 configures a fixed routing table between each network interface to process the static routing. In this case, the routing table cannot be dynamically changed by the routing protocol, and specific routing services will be provided according to the pre-set routing policy.
- Dynamic Routing – The OfficeServ 7200 supports routing information exchange protocols to react to the changing network environment more effectively:
  - RIPv1, RIPv2: These protocols are widely used for managing the routing information in a mid-sized independent network such as a group of LANs
  - OSPFv2: This protocol is used in a large-sized independent network. A router detects and reports any change in the routing table or the network to other routers, thus all routers share the same routing information.
- Performs inter-VLAN routing – Communication between the VLAN groups.

Data Network Security

- Outbound and Inbound NAT/PT
  - Controls an access to internal resources through conversion between the Global IP and Private IP. Network Address Translation and Port Address Translation services protect devices on the private internal LAN from being exposed on the Public Network. This service also allows a single public IP address to be shared among multiple hosts on the internal LAN.
- Firewall
  - Access Filtering: Access lists and policies can be implemented to control access to the Data Server resources.
  - DMZ Function: Hosts connected to the DMZ port can bypass the network firewall making it easier for external clients to access their services. Applications such as web servers and mail servers are typically connected to the DMZ ports.
  - Port Forwarding: This feature allows external hosts on the public network to access hosts and services on the internal private LAN by forwarding the public WAN address to a private LAN address based on a specific port

© SAMSUNG Telecommunications America, L.P.

- Intrusion Detection System(IDS)
  - Detects and notifies an access to unauthorized areas by the access list.
  - Recognizes and notifies unauthorized packets by applying the basic intrusion rule for packets.
  - Detects and blocks DoS attacks such as SYN flood.
- Virtual Private Network(VPN)
  - The VPN capability creates encrypted 'tunnels' through the Internet, allowing branch offices or remote users to securely connect into the network from off-site.
  - Functions as a VPN gateway based on PPTP and IPSec.
  - Performs privacy and integrity through VPN tunneling and data encryption.

Data Network Application

Functions as data network applications such as NAT/PT, Firewall, VPN, DHCP, and Application Level Gateway(ALG)

- SIP Aware Application Level Gateway (ALG)
  - This feature takes SIP packets coming to the WAN interface and redirects them to any SIP user agents connected to the private LAN.
- DHCP Server
  - This service dynamically assigns IP addresses to all hosts connected to the private LAN.

QoS

- Processes priority for layer 2 frames based on the 802.1p standard(Switch function)
- Processes priority queuing for layer 3 packets and for selected IPs. The ToS (Type of Service) field of the IP header is checked and process according to the priority of the corresponding routing in the data server.
- Processes priority queuing for layer 4 packets and for RTP packets (UDP/TCP port). Prioritize RTP voice packets over normal data packets for improved voice quality in VoIP applications.

DSMI

- This service automatically configures the router to allow for VoIP applications such as remote IP phones and IP networking, IP Trunking, etc. If the OfficeServ 7200 VoIP services provided by MCP and MGI use private IP, and they are connected behind the WIM router's public IP, DSMI will automatically perform NAPT for signaling and media data packets for VoIP services.

Management

- Supports a specialist level debugging function through Telnet connection
- Supports configuring and verifying the functional block operations of the data server through a web-based browser
- Exchanges IDS data and alarm data with the system manager
- Program upgrade
  - Upgrades program through TFTP
  - Upgrades program through HTTP

© SAMSUNG Telecommunications America, L.P.

CHAPTER 2. OfficeServ 7200 Data Server Installation

This chapter describes the installation and login procedures for the OfficeServ 7200 Data Server.

Installation Procedure

OfficeServ 7200 Data Server software is installed on WIM board. The software package is composed of items described below:

Package	File	Description
Bootrom Package	bootldr.img-vx.xx bootldr.img-vx.xx.sum	Boot ROM program
Main Package	ds-pkg-vx.xx.tar.gz	Upgrade package for HTTP on the WEB Management
	app.img-vx.xx app.img-vx.xx.sum	'app' partition upgrade package for TFTP
	config.img-vx.xx config.img-vx.xx.sum	'config' partition upgrade package for TFTP
	kernel.img-vx.xx kernel.img-vx.xx.sum	'kernel' partition upgrade package for TFTP
	log.img-vx.xx log.img-vx.xx.sum	'log' partition upgrade package for TFTP
	ramdisk.img-vx.xx ramdisk.img-vx.xx.sum	'ramdisk' partition upgrade package for TFTP
	flash1.img-vx.xx flash1.img-vx.xx.sum	The first flash fusing file
	flash2.img-vx.xx flash2.img-vx.xx.sum	The second flash fusing file

Software Package Configuration

Each package has a separate file for checking checksum, and x.xx represents the version.

Setup the environment as follows to access the Data Server.

1. Mount the WIM board on slot 1 and the LIM board on slot 2.
   - In order to connect the WIM board to the LIM board through the back panel, first place the shunt pin of JP1, 2, 3, and 4 toward the back of the WIM board, then mount the WIM board to the back panel direction.

© SAMSUNG Telecommunications America, L.P.

- If the shunt pin of JP1, 2, 3, 4 is directed to the front of the WIM board, connect the LAN port of the WIM board to one of the Ethernet port of the LIM board through a LAN cable.

2. Connect a PC to a Ethernet port of the LIM board.

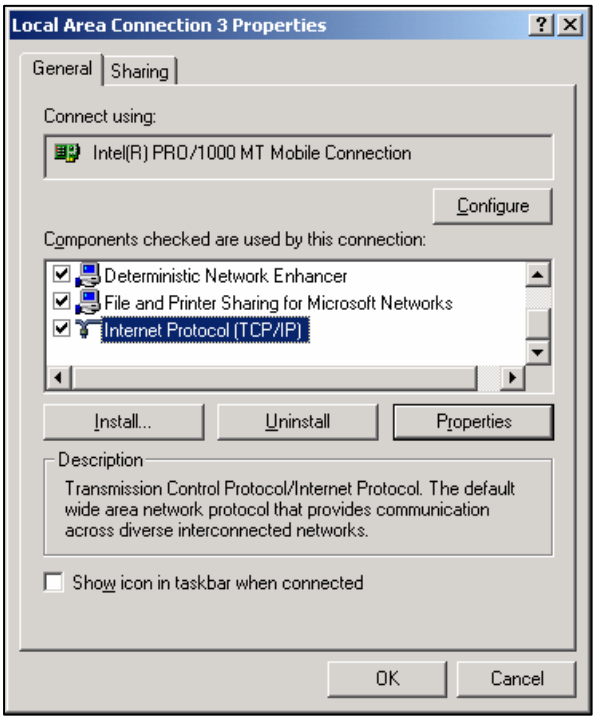
Configuring the PCs

This section describes how to configure your PC to communicate with the OS 7200 Data Server Management Web Browser.

The instructions below apply only to Windows 2000 or XP computers. Make sure that an Ethernet card or adapter has been successfully installed in your PC.

1. Click the [Start]button. Click [Settings] and then [Control Panel]. From there, double-click the [Network] icon.

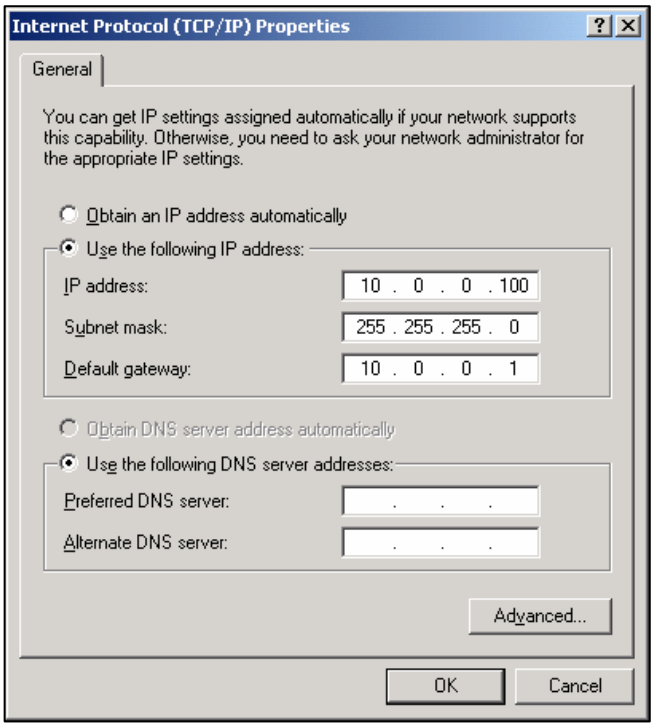
2. On the [Configuration] tab, select the **Internet Protocol (TCP/IP)** line for the applicable Ethernet adapter. Click the [Properties] button.



3. Click the [IP Address] tab and select **Specify an IP address**. Enter the following IP address:

   - IP Address: Enter a unique IP address that is not used by any other computer on the network connected to the OS 7200 data server. You can use an IP address in the ranges of 10.0.0.2 to 10.0.0.254.
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 10.0.0.1 (OS 7200 Data Server's default IP address)

   Click the [OK] button in the Internet Protocol Properties window. Click the [OK] button in the Local Area Connection Properties window.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 0 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

4. Execute the Internet Explorer from the PC and connect to the IP of LAN. The default IP address of the WIM board managing the LIM board is set to '10.0.0.1'.

CAUTION

Using Web Browser

Use Microsoft Internet Explorer 6.0 or higher as a Web browser to maintain OfficeServ 7200 Data Server.

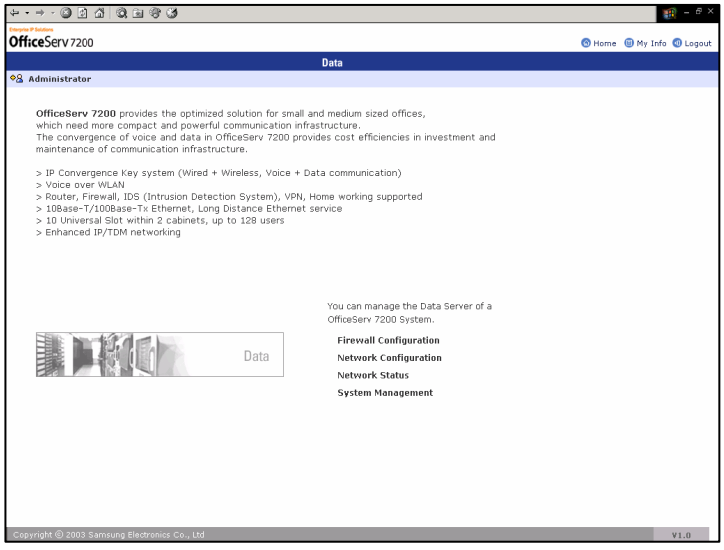
© SAMSUNG Telecommunications America, L.P.

Starting up the OfficeServ 7200 Data Server

The procedure for starting up the OfficeServ 7200 Data Server is as follows:

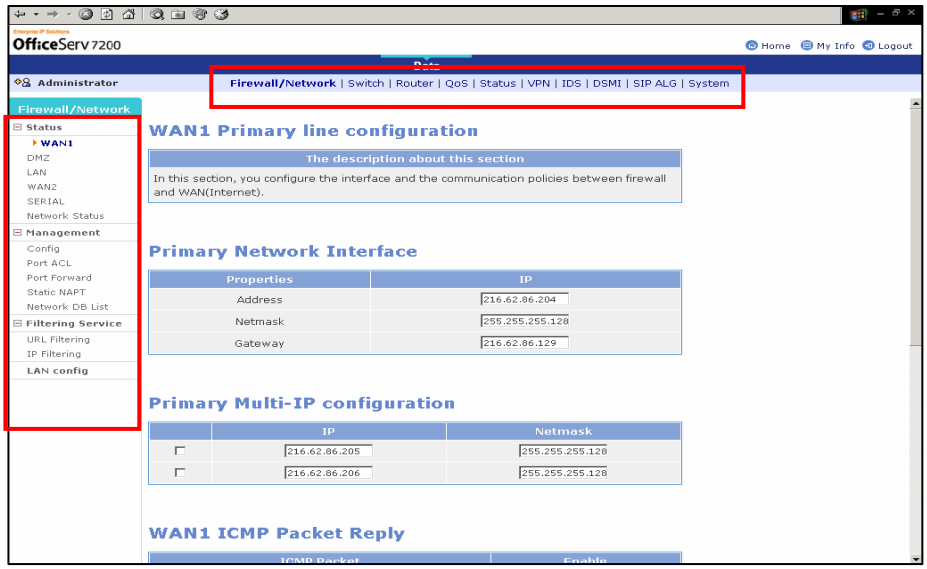
1. Start the Internet Explorer and enter the IP address of the Data Server into the address bar. The login window shown below will appear:

2. Login using the administrator ID and password. The default Login ID and Password are **Admin** and **Admin** respectively. Click the [OK] button to proceed. The following window will appear:


OfficeServ 7200
Home
My Info
Logout
Data
Administrator
OfficeServ 7200 provides the optimized solution for small and medium sized offices, which need more compact and powerful communication infrastructure.
The convergence of voice and data in OfficeServ 7200 provides cost efficiencies in investment and maintenance of communication infrastructure.
> IP Convergence Key system (Wired + Wireless, Voice + Data communication)
> Voice over WLAN
> Router, Firewall, IDS (Intrusion Detection System), VPN, Home working supported
> 10Base-T/100Base-Tx Ethernet, Long Distance Ethernet service
> 10 Universal Slot within 2 cabinets, up to 128 users
> Enhanced IP/TDM networking
You can manage the Data Server of a OfficeServ 7200 System.
Data
Firewall Configuration
Network Configuration
Network Status
System Management
Copyright © 2003 Samsung Electronics Co., Ltd
V1.0

3. Click [Data] to use the menus for Data Server shown in the following window:

When a 'Data' menu is selected, the submenus of the Data Server menu appear on the left section of the window. Descriptions on each submenu are provided in 'Chapter 3. Using the OfficeServ 7200 Data Server'.



CAUTION

Delete Temporary Internet Files

Delete Temporary Internet Files after upgrading Data Server package.

Select the [Internet Explorer] → [Tools] → [Internet Options] menu, click the [Delete Cookies] and the [Delete Files] button in the [Temporary Internet files].

If the Temporary Internet Files are not cleared, Data Server Web Management displayed info will not be correct.

© SAMSUNG Telecommunications America, L.P.

CHAPTER 3. Using the OfficeServ 7200 Data Server

This chapter describes how to use the menus of the OfficeServ 7200 Data Server.

The menus of the OfficeServ 7200 Data Server are as follows:

Firewall/Network Menu

Firewall/Network Menu provides a Configuration Wizard to setup the WAN1, WAN2, LAN, DMZ, and Serial network interfaces, as well as firewall and the communication policies between the firewall and each interface. Under this menus, you can also setup the Data Server Access Control List, Port Forward, and Filtering Services.

Select [Firewall/Network] to display the submenus of Firewall/Network on the upper left section of the window.

Menu	Submenu	Description
Status	WAN1	Displays user settings of the WAN1 port, which is an external port used for Internet connection.
	DMZ	Displays user settings of the DMZ port, which is an internal port. The DMZ (Demilitarized Zone) allows internal LAN devices to be accessible to Internet traffic, such as Web servers, FTP servers.
	LAN	Displays user settings of the LAN port, which is an internal port.
	WAN2	Displays user settings of the WAN2 port, which is an external port.
	SERIAL	Displays user settings of the SERIAL port, which is an external port.
	Network status	Displays a summary of status of all ports.

© SAMSUNG Telecommunications America, L.P.

Menu	Submenu	Description
Management	Config	Sets firewall and network interface configuration.
	Port ACL	Allows external users to access OS 7200 firewall.
	Port Forward	Sets port forward to pass thru OS 7200 firewall. The incoming traffic is directed to specific local PCs based on one specified destination port number.
	Static NAPT	Sets port forward to pass thru OS 7200 firewall. The incoming traffic is directed to specific local PCs based on a range of service port numbers.
	Network DB List	Deletes DB where settings are saved.
Filtering Service	URL Filtering	Blocks the internal network web access to the URL name setting.
	IP Filtering	Blocks the internal network web access to the IP setting.
LAN config	-	Sets the transfer rate and transmission system of Ethernet port.

© SAMSUNG Telecommunications America, L.P.

Status

The [Status] menu displays the setting of the WAN1, DMZ, LAN, WAN2, or SERIAL.

NOTE

Port Setup Procedure

The WAN1, LAN, DMZ, WAN2, and SERIAL ports are set at the [Firewall/Network] → [Management] → [Config] menu. Refer to the description on the menu for the setup procedures.

WAN1

The [Status] → [WAN1] menu shows the setting of WAN1, which is an external port using a public IP.

NOTE

Port Settings

Refer to descriptions on the [Firewall/Network] → [Management] → [Config] menu for details on the items of the setting.

DMZ

The [Status] → [DMZ] menu shows the setting of DMZ, which is an internal port using a private IP or public IP.

LAN

The [Status] → [LAN] menu shows the setting of LAN, which is an internal port using a private IP.

WAN2

The [Status] → [WAN2] menu shows the setting of WAN2, which is an external port using a public IP.

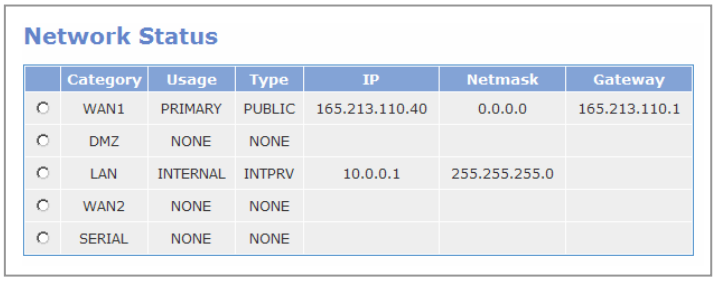
SERIAL

The [Status] → [SERIAL] menu shows the setting of SERIAL, which is an external port using a public IP.

DMZ, LAN, WAN2, and SERIAL ports' settings
Settings of ports that have no lines connected (When the port is set to 'Not Used'at the [Management] → [Config] menu) are displayed as 'No line's connected to this port'.

Network Status

The [Status] → [Network Status] menu displays the current IP Address of WAN1, DMZ, LAN, WAN2, and SERIAL.



Item	Description
Category	WAN1, DMZ, LAN, WAN2, and SERIAL ports
Usage	- NONE: Unused line - PRIMARY: Primary public interface - SECONDARY: Secondary public interface - INTERNAL: Line used for internal interface
Type	- NONE: Not used port - PUBLIC: Port using public IP - INTPRV: Internal port using private IP - INTDMZ: Internal DMZ port

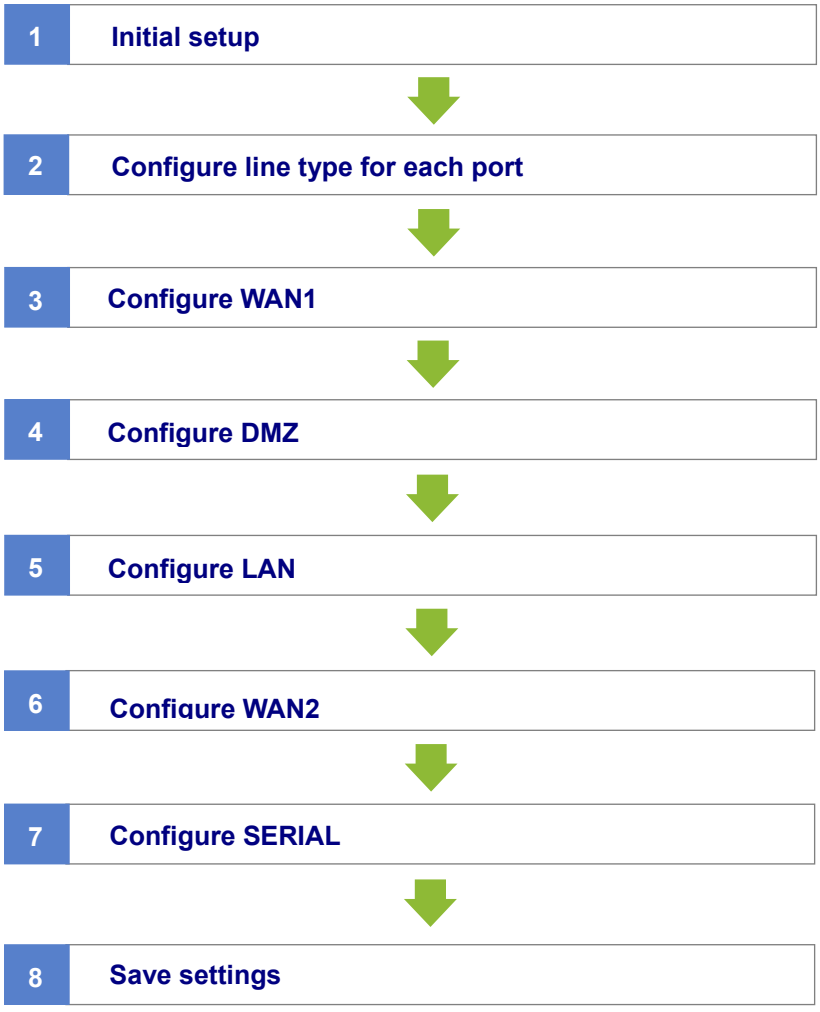
© SAMSUNG Telecommunications America, L.P.

Management

The [Management] menu sets ports related to firewall and network.

Config

The [Config] menu starts the configuration wizard which will guide through the settings of the WAN1, LAN, DMZ, WAN2, and SERIAL ports. Select [Management] → [Config] and set the items of each window. Click the [Next] button and set the firewall and network according to the following procedure:

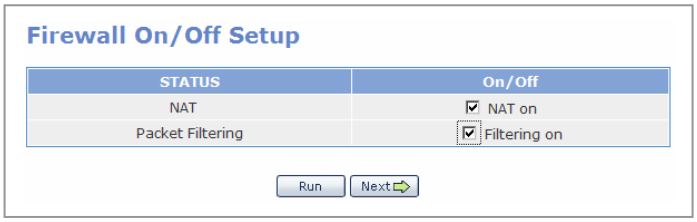


© SAMSUNG Telecommunications America, L.P.

Initial Setup

1. Select [Management] → [Config] and display the window shown below. The 'NAT' and 'Packet Filtering' items are originally disabled. Check the checkboxes to set the status to 'On' and click the [Run] button.

   If these items are checked, Click the [Next] button.



NOTE

Network Address Translation (NAT)

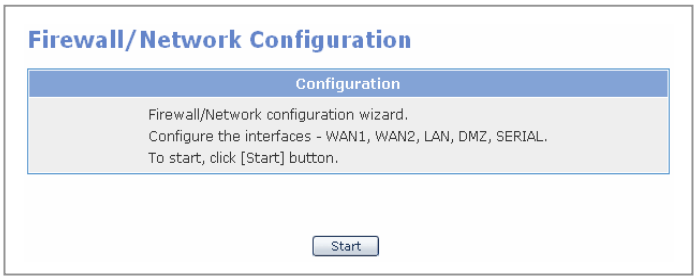
NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. NAT adds a level of security by protecting the address of a PC connected to the private LAN from transmitted on the Internet. If only a single Internet IP address is provided by the ISP (such as a DSL or cable modems internet account), NAT must be selected to allow all PCs on the LAN to share this single Internet IP address.

NOTE

Packet Filtering

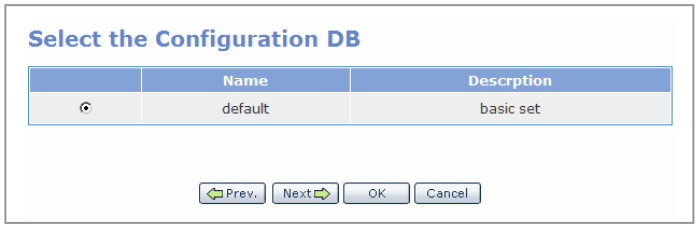
Packet Filtering controls access to the local-area network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

2. Click the [Start] button to start the Firewall/Network configuration wizard, which will step through configuration for each interface.



© SAMSUNG Telecommunications America, L.P.

3. New settings can be set or previously set setup files can be changed or executed from the following window. The IP of the LAN port is initially set to '10.0.0.1'. Check the 'default' item and click the [Next] button.



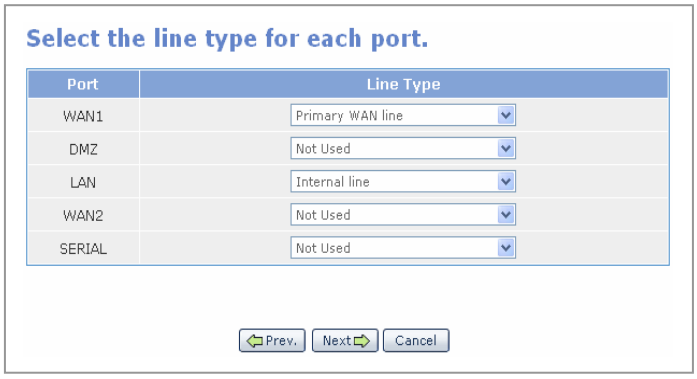
Set Line Type for Each Port

External ports (e.g., WAN1, WAN2, SERIAL) use public IPs while internal ports (e.g., DMZ, LAN) use public or private IPs. Select the line type for each port as listed below:

- External port (WAN1,WAN2, SERIAL)
  - Primary WAN line: Primary internet connection interface
  - Secondary WAN line: Secondary internet connection interface
  - Third WAN line: Third internet connection interface
  - Not Used: No WAN line is connected

- Internal port (DMZ, LAN)
  - Internal line: Internal line is used
  - Not Used: Internal line is not used

In the figure shown below, WAN1 port is set to Primary WAN line as the primary line, LAN port is to Internal line as the internal line, and WAN2, SERIAL, and DMZ ports are set to Not Used as lines not connected:



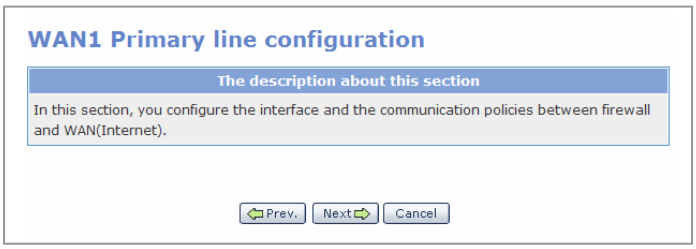
CAUTION

Dynamic IP Address (e.g. Cable Modem, ADSL PPPoE, and SDSL internet account)
If a dynamically assigned IP address is used for WAN internet connection, information (e.g., 'Port Forward' and 'Static NAPT') on public IPs will not be automatically changed. 'Fixed IP' should be used for VoIP services that require settings of the 'Port Forward' and 'Static NAPT' menus and for VPN services that require WAN IP address setting.

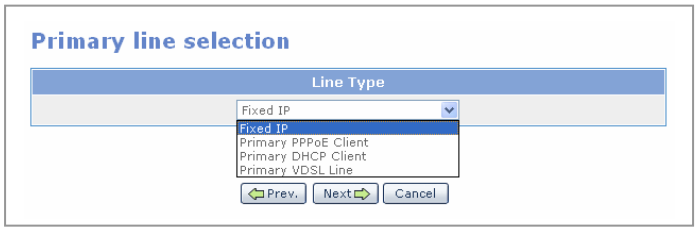
© SAMSUNG Telecommunications America, L.P.

WAN1 Setup

1. The starting window for setting WAN1 as "Primary WAN line' is shown below. Click the [Next] button to start setting the WAN1 port.


WAN1 Primary line configuration
The description about this section
In this section, you configure the interface and the communication policies between firewall and WAN(Internet).
Prev.
Next
Cancel

2. Select the line type for Primary WAN line. Select one of the four applications shown below for the external network:



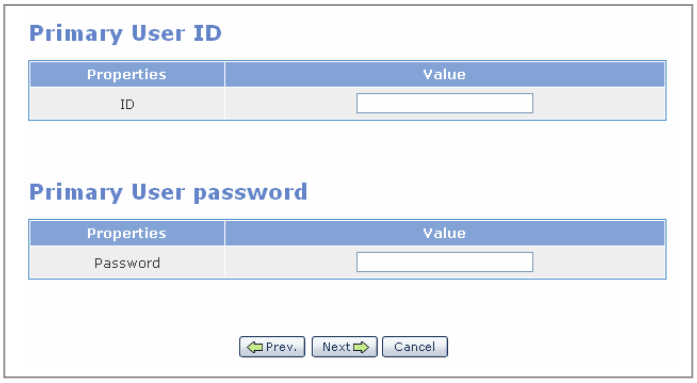
Fixed IP: Select Fixed IP if your Internet service account uses Fixed IP (Static) IP assignment.

- Primary PPPoE Client: Select Primary PPPoE Client if your Internet service account uses PPP over Ethernet login protocol, such as in ADSL account.
- Primary DHCP Client: Select Primary DHCP Client if your Internet service account uses Dynamic IP assignment, such as in Cable Modem account.
- Primary VDSL Line: Select Primary VDSL Line if your Internet service account uses VDSL service.

The four applications of Primary WAN line are described below:

a. Fixed IP: Enter values in the Address, Netmask, and Gateway fields to perform settings in the WAN1 port on an external network where a static IP is used, and click the [Next] button. To add another IP, apart from the IP of the external line currently being used, click the [Add] button and add the item. OfficeServ 7200 WAN interface supports up to eight multiple public IP addresses.

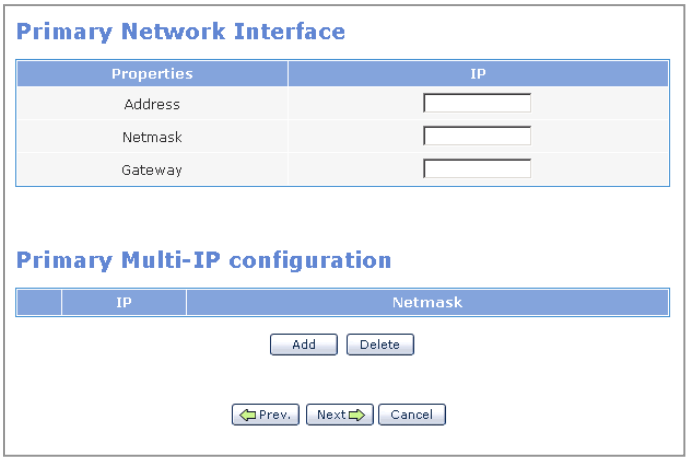
© SAMSUNG Telecommunications America, L.P.



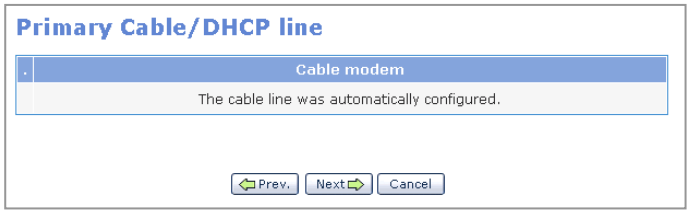
Caution Against Changing Network Interfaces

If a network interface configuration (e.g., IP, gateway, and subnet mask) is changed during router regular operation, all the active IP sessions that are connected in the router will be disconnected.

b. Primary PPPoE Client: Enter the ID and password to connect an external network where a dynamic IP will be assigned through PPPoE, and click the [Next] button.



c. Primary DHCP Client: Connect to internet network using a cable modem or a DHCP server, the port is automatically set. Click the [Next] button and proceed to the next window.

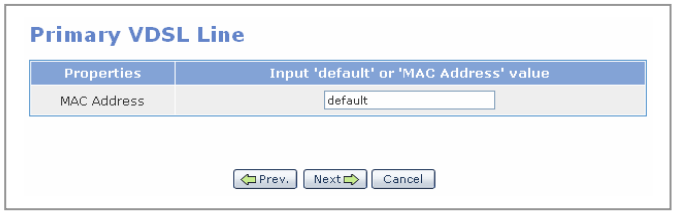


NOTE

PPPoE/DHCP/SDSL Settings

The performance of data uploading or downloading speed depending on Internet Service Provider services.

d. Primary VDSL line: External network using a VDSL modem.
Enter 'default' into the 'Mac address' field to disable MAC authentication, and click the [Next] button. Enter a MAC address into the 'Mac address' field to use the MAC copy function.



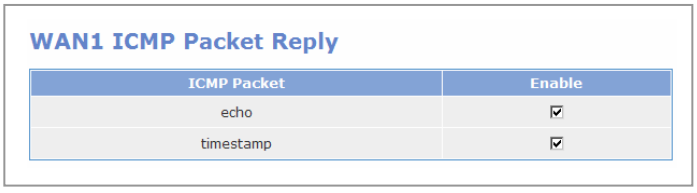
NOTE

MAC Copy Function

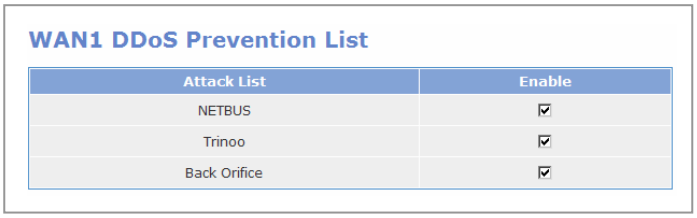
When performing authentication through PC MAC of LIM board, MAC of outgoing packets are copied to PC MAC instead of using MAC of outgoing packets as MAC of WAN1.

3. Select the items below and clock the [Next] button:

- **WAN ICMP Packet Reply**: The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet protocol suit. ICMP Echo and Timestamp messages are used for network diagnostics, often to test the availability of a target, such as the popular 'ping' program. Many malicious attacks begin with a ping scan. Disabling ICMP Packet Reply prevents your system's discovery with a ping. OfficeServ 7200 firewall does not respond to ICMP echo and ICMP timestamp by default. However, if the 'echo' and 'timestamp' items are checked, response to external Ping commands will be displayed. If these items are not checked, a Request timed out will occur to external Ping commands.

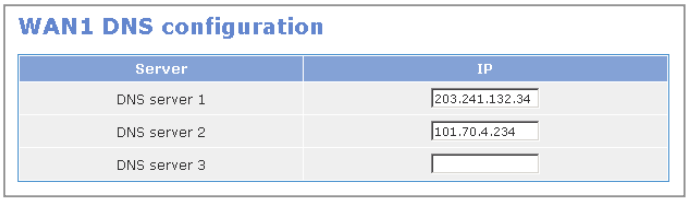


- **WAN1 DDos prevention**: Check the items shown below to prevent DDoS (Denial of Service) attacks by blocking attacks using the corresponding hacking programs.



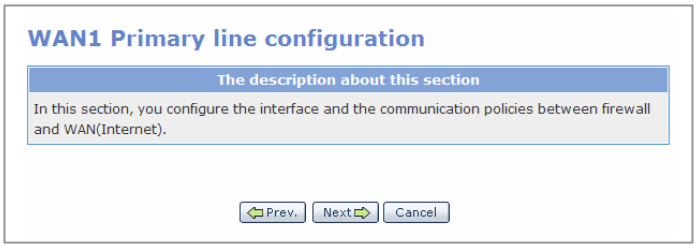
© SAMSUNG Telecommunications America, L.P.

- **WAN1 DNS configuration**: Enter the IP address of the DNS server. If PPPoE/DHCP is used, there is no need to manually enter these fields, ISP will automatically authenticate the DNS servers.

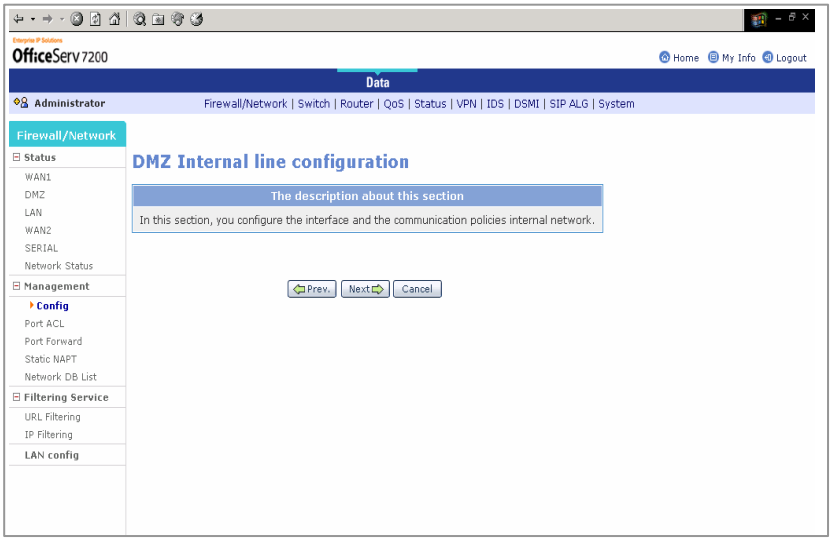


DMZ Setup

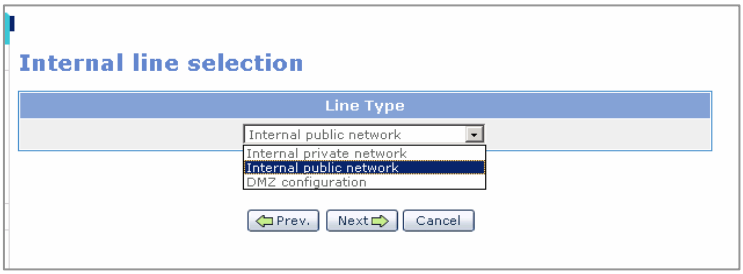
1. The starting window for setting WAN1 as "Primary WAN line' is shown below. Click the [Next] button to start setting the WAN1 port.


WAN1 Primary line configuration
The description about this section
In this section, you configure the interface and the communication policies between firewall and WAN(Internet).
Prev.
Next
Cancel

2. The starting window for setting DMZ 'Internal Line' configuration is shown below. Click the [Next] button and proceed to start setting the DMZ port.



3. Select the line type for the DMZ line. Select one of the three applications shown below for the DMZ port.



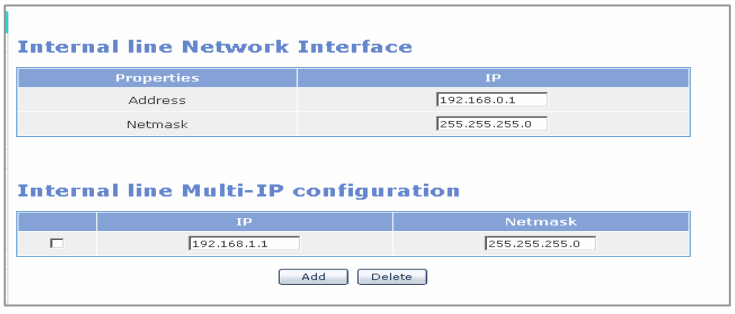
DMZ port supports the following three line type:

a. Internal private network: Use DMZ port as a second private LAN network behind the router's firewall.
b. Internal public network: Place DMZ port behind the router in the private network, but assign it with a public IP address to allow DMZ port accessible from the public network.
c. DMZ configuration: Configure DMZ port with a private IP address and use the OfficeServ 7200 NAT router to allow DMZ port accessible from the public network.

The configurations of each DMZ line type are described below:

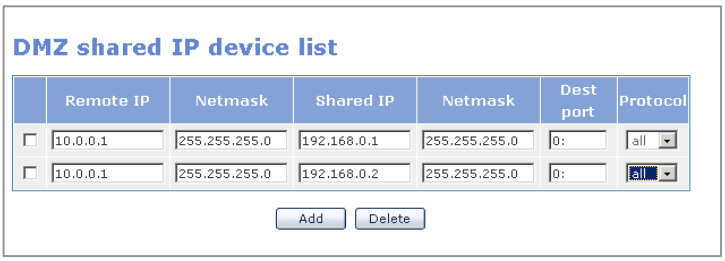
- Internal private network: Assign DMZ port with the private IP address in the Address, and Netmask, fields. If additional private IP addresses with different subnet are currently being deployed, click the [Add] button to add the items. OfficeServ 7200 allows up to 4 subnets in the 'Internal line Multi-IP configuration'.

  In the example shown below, two DMZ IP of 192.168.0.1/24 and 192.168.1.1/24 are set.



  Under the **DMZ shared IP device list**, configure the devices from the LAN interface that can send packets to pass through the DMZ interface and access the DMZ servers.

In the example shown below, allow the LAN interface as entered in the 'Remote IP' to access the DMZ servers as entered in the 'Shared IP'. The Destination Port of '0:' indicates all ports are allowed for access.



NOTE

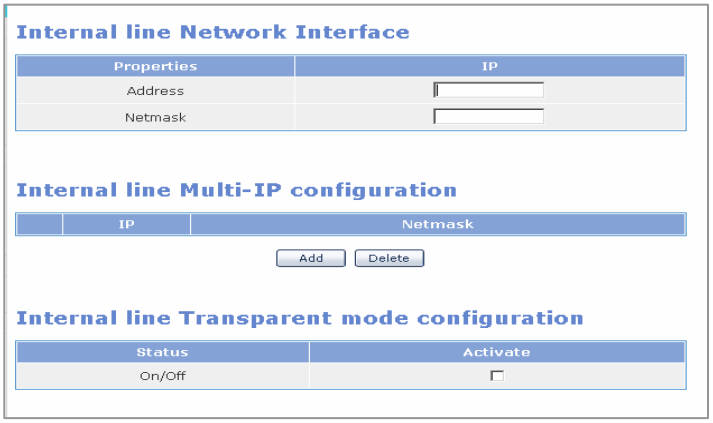
Port Range Setting

- When using ports from 0 to 100, enter '0:100'.
- '0:' indicates all ports.

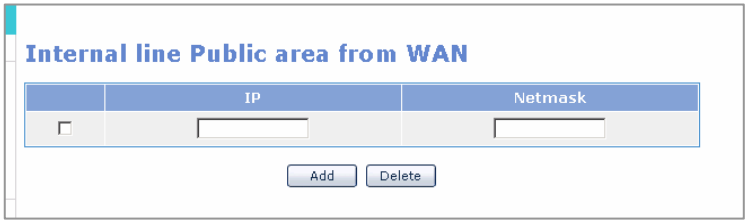
- Internal public network: Assign DMZ port public IP address under the Internal Line Network Interface and Internal Line Multi-IP Configuration.

  In this scenario, the DMZ port with a public IP address is hiding on a private network behind a router, and still have appearance of being on the public network 'in front of ' the router.

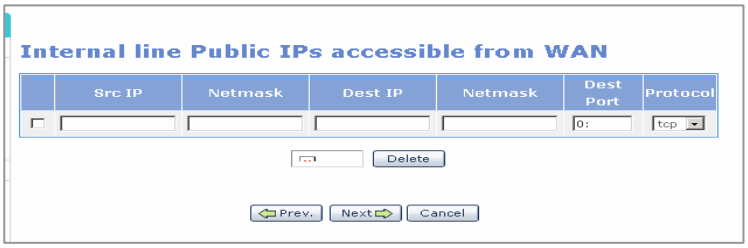
  If the checkbox of 'Internal line Transparent mode configuration' is selected, the servers on the DMZ network use the external public IP as the default gateway. If 'Internal line Transparent mode configuration' is deactivated, the servers on the DMZ network use the DMZ port as the default gateway.



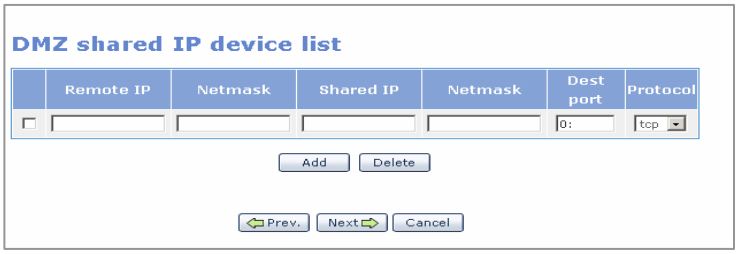
Configure **Internal line Public area from WAN** for hosts that use DMZ as an internal public network, and click the [Next] button.



Configure **Internal line Public IPs accessible from WAN** to allow external networks to access a specific server on the DMZ network inside the firewall that has a public IP.

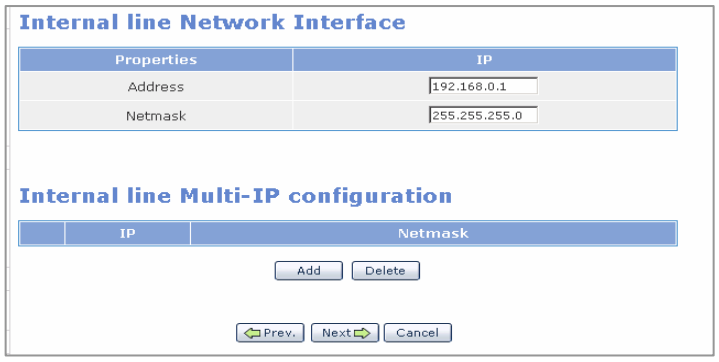


Under the **DMZ shared IP device list**, configure the devices from the LAN interface that can send packet to pass through the DMZ firewall and access the DMZ servers.



- DMZ Configuration: Enter Private IP address values in the Address, and Netmask, fields. If additional private IP address is currently being deployed, click the [Add] button to add the items.

In the example shown below, DMZ IP of 192.168.0.1/24 is set.



Under the **Internal line DMZ configuration**, configure the servers on the DMZ network.

Enable port forwarding of a specific packet received through WAN public network to a host located in DMZ.

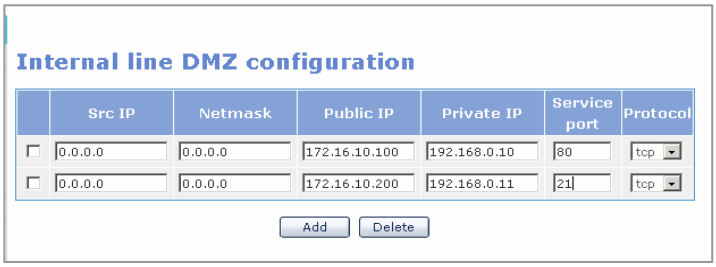
- Src IP: Enter the source IP of a packet from public network to be forwarded to a port.
- Netmask: Enter the netmask of a packet to be forwarded to a port.
- Public IP: Enter the IP address of WAN.
- Private IP: Enter the IP address of a host located in DMZ.
- Service Port: Enter the number of a port to which a packet is forwarded.
- Protocol: Select the type of a protocol to be forwarded.

In the example show below, the following two servers are connected on the DMZ network:

- Web server with private IP address of 192.168.0.10 and service port of 80
- FTP server with private IP address of 192.168.0.20 and service port of 21

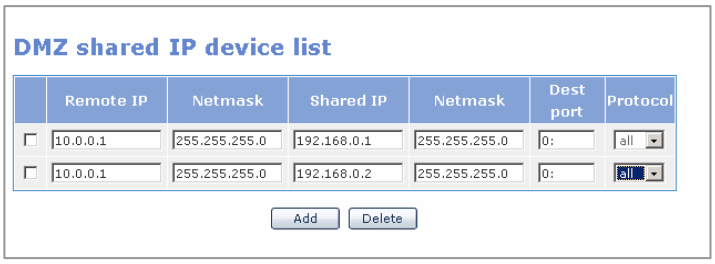
The Source IP address and Netmask are set to 0.0.0.0 to allow all the devices in the public network to access these two DMZ servers.

Click the [Next] button to move to the next step.



Under the **DMZ shared IP device list**, configure the devices from the LAN interface that can send packets to pass through the DMZ and access the DMZ servers.

In the example shown below, allow the LAN interface as entered in the ‘Remote IP’ to access the DMZ servers as entered in the ‘Shared IP’. The Destination Port of ‘0:’ indicates all ports are allowed for access.

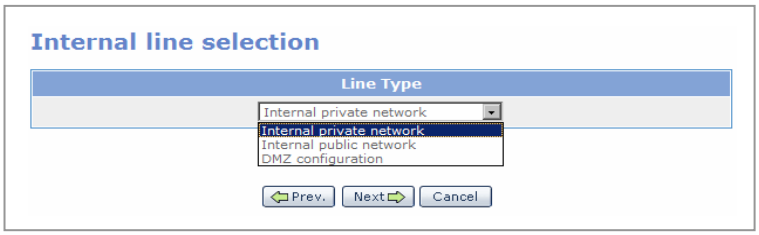


LAN Setup

1. The below window shows the LAN was set to 'Internal line' at the <Select the line type for each port> window. Click the [Next] button to start LAN port setup.

LAN Internal line configuration
The description about this section
In this section, you configure the interface and the communication policies internal network.
Prev.
Next
Cancel

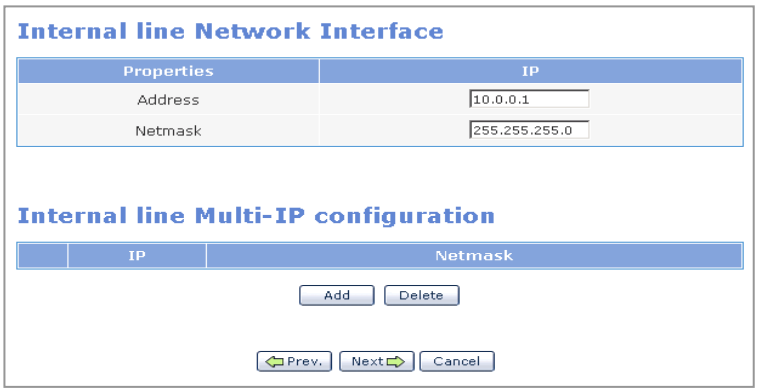
2. Select the internal line type.



Types of internal lines are described below:

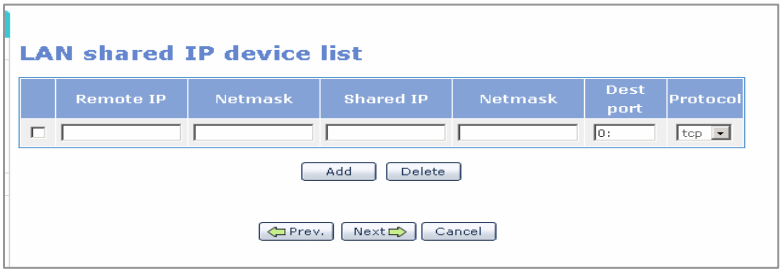
- Internal private network: Select this option to configure an internal network using a private IP.

  Enter the IP address, Netmask, and Gateway to use LAN as an internal private network, and click the [Next] button. To add another IP, apart from the IP of the internal line currently being used, click the [Add] button and add the item.



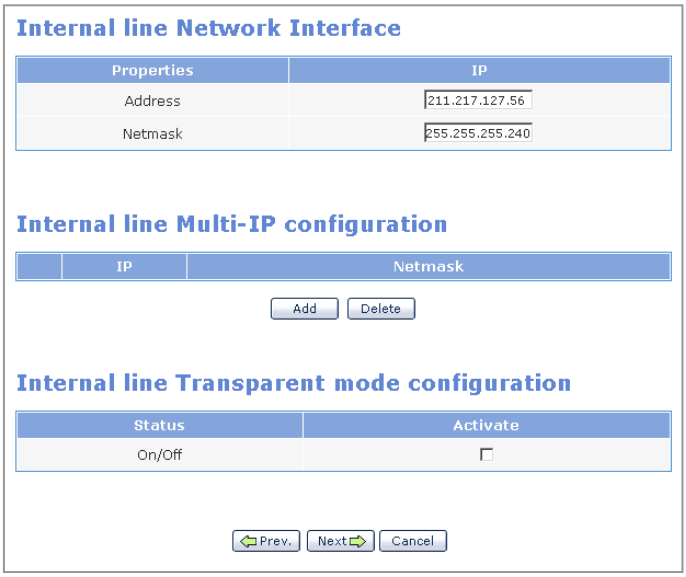
Under the **LAN shared IP device list**, configure the devices from the DMZ interface that can send packets to pass through the LAN firewall and access the LAN servers.

Enter the DMZ interface as entered in the 'Remote IP' and enter the LAN servers to be shared in the 'Shared IP'. The Destination Port of '0:' indicates all ports are allowed for shared IP Device

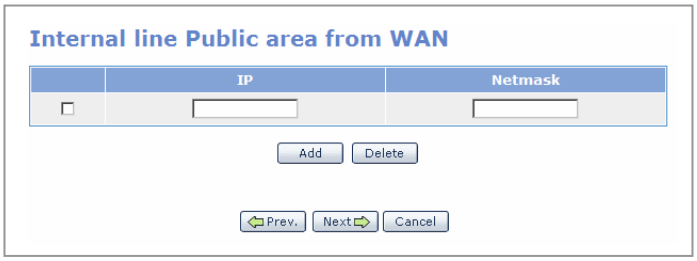


- Internal public network: Select this option to configure an internal network using a public IP. Click [Add] to add an IP in addition to the IPs of the internal line being used.

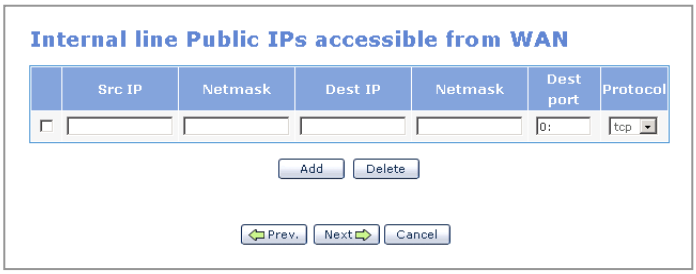
If the checkbox of '**Internal line Transparent mode configuration**' is selected, the servers on the LAN network use the external public IP as the default gateway. If 'Internal line Transparent mode configuration' is deactivated, the servers on the LAN network use the LAN port as the default gateway.



Configure **Internal line Public area from WAN** for hosts that use LAN as an internal public network, and click the [Next] button.



Configure **Internal line Public IPs accessible from WAN** to allow external networks to access a specific server on the LAN network inside the firewall that has a public IP.

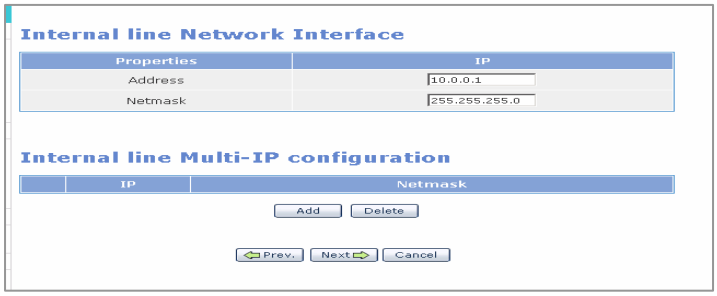


Under the **LAN shared IP device list**, configure the devices from the DMZ interface that can send packets to pass through the LAN firewall and access the LAN servers.

Enter the DMZ interface as entered in the ‘Remote IP’ and enter the LAN servers to be shared in the ‘Shared IP’. The Destination Port of ‘0:’ indicates all ports are allowed for shared IP Device

- DMZ configuration: Enter Private IP address values in the Address and Netmask fields. If additional private IP address is currently being deployed, click the [Add] button to add the items.

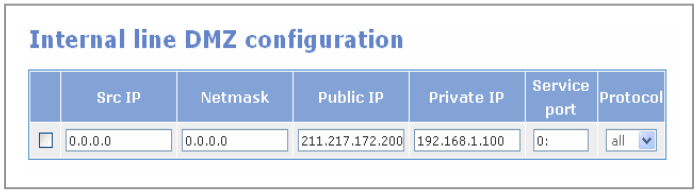
In the example shown below, LAN IP of 10.0.0.1/24 is set.



Under the **Internal line DMZ configuration**, configure the servers on the LAN network. Enable port forwarding of a specific packet received through WAN to a host located in LAN.

- Src IP: Enter the source IP of a packet to be forwarded to a port.
- Netmask: Enter the netmask of a packet to be forwarded to a port.
- Public IP: Enter the IP address of WAN.
- Private IP: Enter the IP address of a host located in DMZ.
- Service Port: Enter the number of a port to which a packet is forwarded.
- Protocol: Select the type of a protocol to be forwarded.

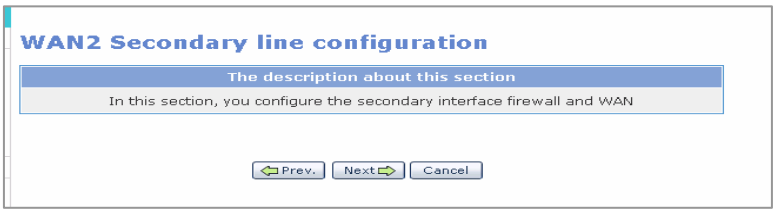
The following window illustrates an example of forwarding all packets (Src IP: 0.0.0.0, Network: 0.0.0.0, Service Port: 0, Protocol: all) that enters the WAN Interface IP (211.217.172.200) to a host (192.168.1.100) located in DMZ:



Under the LAN shared IP device list, configure the devices from the DMZ interface that can send packets to pass through the LAN and access the servers inside the LAN port. Click the [Next] button.

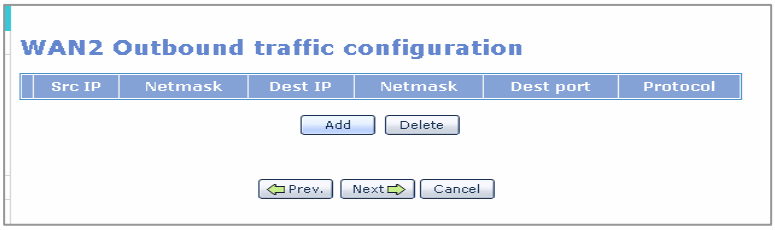
WAN2 Setup

1. If WAN2 was set to Primary WAN line, secondary WAN line, or Third WAN line, click [Next] button to proceed with the WAN2 Setup procedures.



2. Follow the same setup procedures as described in WAN1 setup procedures.

3. Configure **WAN2 Outbound traffic configuration** to specify packets that could be sent from LAN or DMZ interfaces via WAN2 interface.



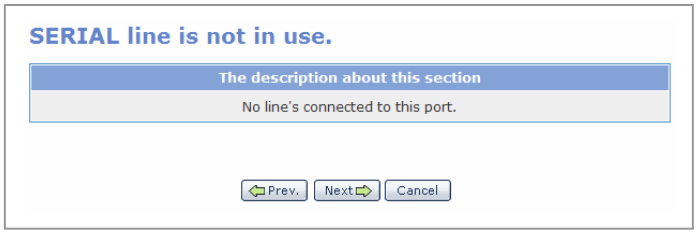
4. Configure **WAN2 Exceptional outbound traffic configuration** to specify packets that are sent from LAN or DMZ interface to be restricted from WAN2 interface.

© SAMSUNG Telecommunications America, L.P.

SERIAL Setup

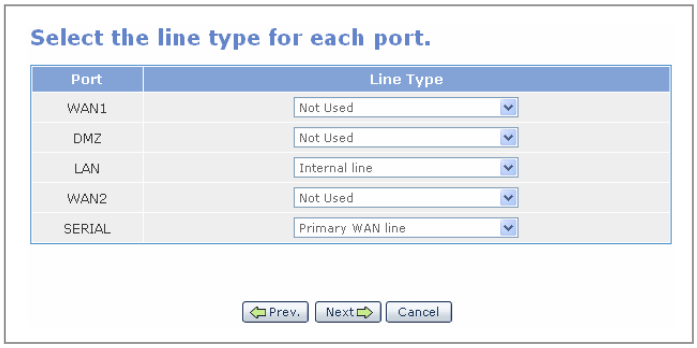
The below window shows that SERIAL was set to 'No line' at the <Select the line type for each port> window (Refer to 'Set Line Type for Each Port').

Click the [Next] button and proceed to the next window.

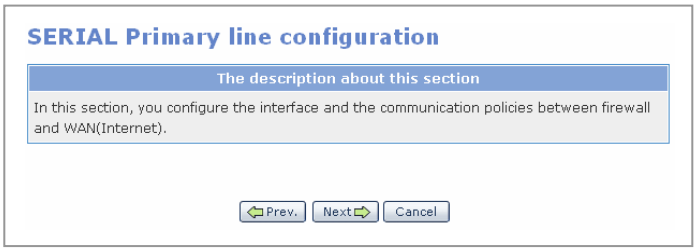


Follow the procedure below to use SERIAL as the Primary WAN line:

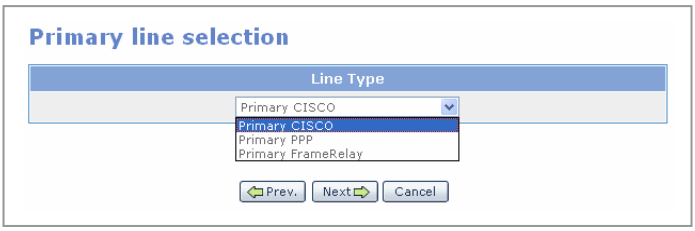
1. Set the SERIAL to 'Primary WAN line' at the <Select the line type for each port> window (Refer to 'Set Line Type for Each Port'), and click the [Next] button.



2. Click the [Next] button to start the SERIAL port setup.

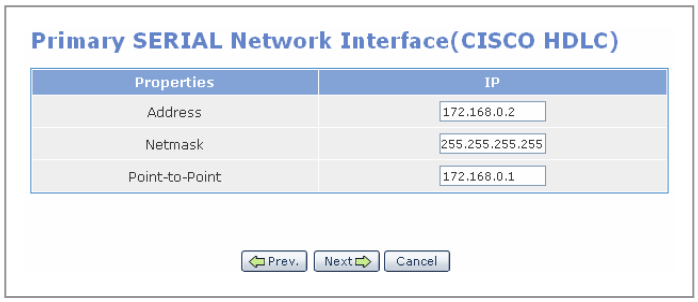

SERIAL Primary line configuration
The description about this section
In this section, you configure the interface and the communication policies between firewall and WAN(Internet).
Prev.
Next
Cancel

3. Select the type of the Primary line.



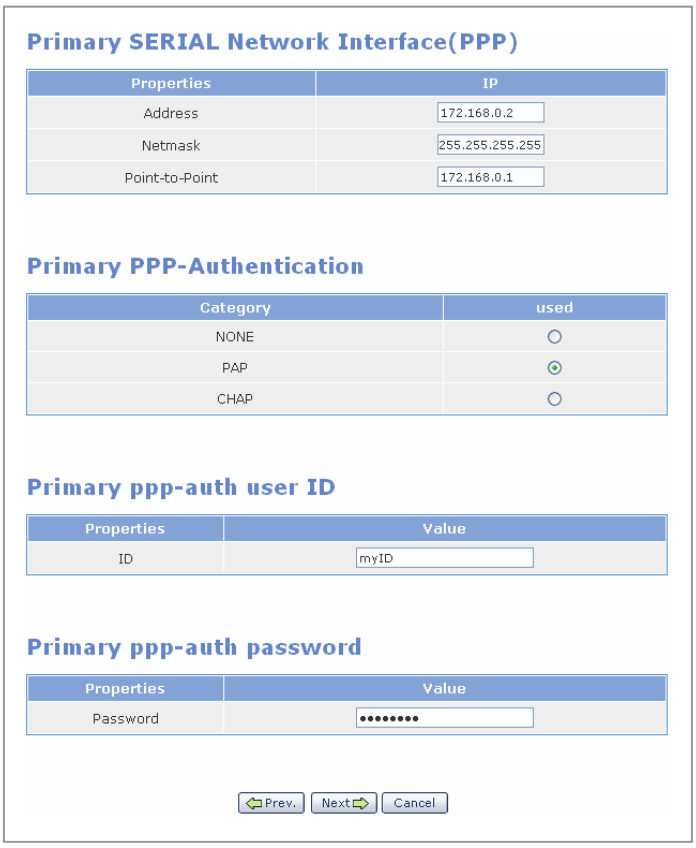
© SAMSUNG Telecommunications America, L.P.

- Primary CISCO: Select ‘Primary CISCO’ from the <Primary line selection> window and click the [Next] button to display the window shown below. Enter the items and click the [Next] button. The CISCO method refers to the HDLC supported by Cisco.



- Primary PPP: Select ‘Primary PPP’ from the <Primary line selection> window and click the [Next] button to display the window shown below. Enter the address, netmask, and point-to-point items.

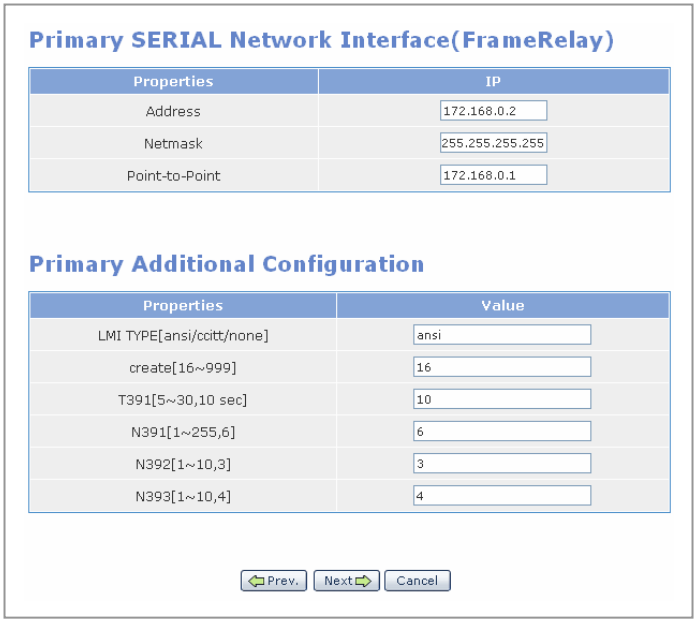
  Select the authentication protocols: None, PAP, or CHAP. Then set the user name and password for the remote router connecting to the router. Click the [Next] button.



  If the Primary PPP-Authentication item is set to ‘NONE’, do not enter the ID and password.

- Primary Frame Relay: Select 'Primary Frame Relay' from the <Primary line selection> window and click the [Next] button to display the window shown below. Enter the items in the Primary SERIAL Network Interface (Frame Relay) and Primary Additional Configuration menus. These values must match the corresponding values set in the frame relay service provider's switch.

  Click the [Next] button.



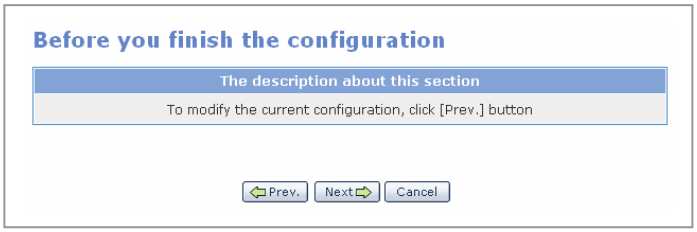
Item	Description
LMI TYPE [ansi, ccitt, none]	Local Management Interface, a signaling standard between the router and the frame relay switch it is connected to. OfficeServ 7200 supports two LMI standards: - ansi: ANSI T1.617 Annex D - ccitt: CCITT
create[16~999]	Range 16~999 Signaling channel No. OfficeServ 7200 supports one Permanent Virtual Circuit (PVC).
T391[5~30,10 sec]	Range 5~30, default is 10 sec. Link Integrity Verification Timer (in seconds). Time interval for DTE to send KeepAlive message.
N391[1~255,6]	Range 1~255, default is 6. Full Status Polling Verification Timer counter, which means the cycle of requesting information on full status based on the number of times that KeepAlive is sent.
N392[1~10,3]	Range 1~10, default is 3. Error threshold counter, the limit of number of repeated errors before the link is marked inactive.

© SAMSUNG Telecommunications America, L.P.

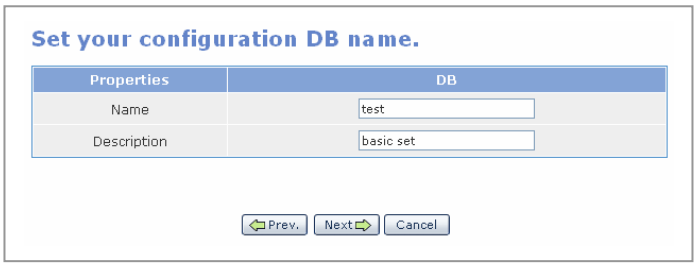
Item	Description
N393[1~10,4]	Range 1~10, default is 4. Monitored Events Counter. When a network becomes active, the number of successful exchanges of KeepAlive messages before the link is considered active.

Saving Settings

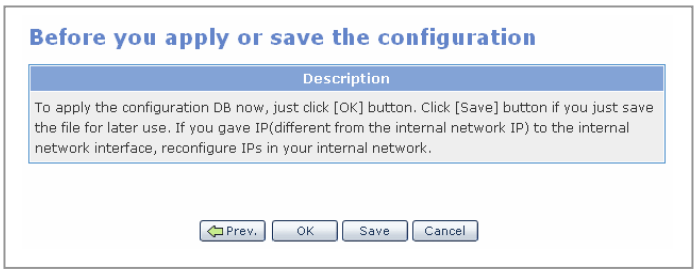
1. The below window shows the firewall and network setup is complete. Click the [Next] button and proceed to the next window.



2. Enter values in the Name and Description fields and click the [Next] button to save the settings in the database. Only uppercase and lowercase alphabet and numbers can be entered in the 'Name' field. Special characters cannot be entered, and 'default' is not available.



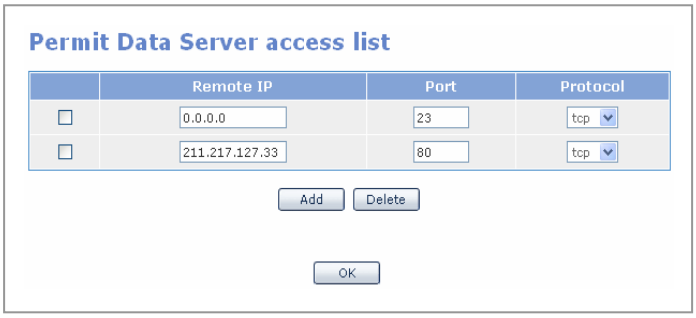
3. Click the [Save] button to save the setting as a file having the file name set above. Click the [OK] button to run the settings upon saving, or click the [Cancel] button the cancel the setting.


Before you apply or save the configuration
Description
To apply the configuration DB now, just click [OK] button. Click [Save] button if you just save the file for later use. If you gave IP(different from the internal network IP) to the internal network interface, reconfigure IPs in your internal network.
Prev.
OK
Save
Cancel

Port ACL

If 'Packet Filtering' in 'Firewall On/Off Setup' is set to 'Filtering on' under [Management] → [Config], external users can not access the OfficeServ 7200 firewall. The [Port ACL] menu is used to allow a specific external IP to access the firewall.

Select [Management] → [Port ACL] and set the IP address, port, and protocol, as shown below, and click the [OK] button:



If the user sets the options as shown above, the server whose IP address is '211.217.127.33' can connect to the system firewall via the web. The external servers can also connect to the firewall by using connection programs such as Telnet and SSH.

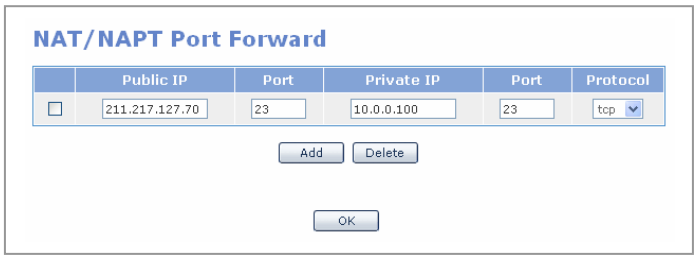
CAUTION

Security Warning

Note that all external users are allowed to access the firewall when the Remote IP is set to '0.0.0.0' and Port is set to '0:'.

Port Forward

The [Port Forward] menu is used to forward packets so that services of the internal server connected to the firewall can be used externally.



For instance, assume that an internal server uses the public IP of the firewall as '211.217.127.70' and the private IP as '10.0.0.100'. If the user uses the telnet server inside the firewall from a server on a network outside the firewall, the user can use telnet services using the Port Forward setting.

Click the [Add] button, and enter values as shown in the above figure. Then, access the telnet server from a network outside the firewall by setting the public IP address to '211.217.127.70' to use telnet services inside the firewall (10.0.0.100).

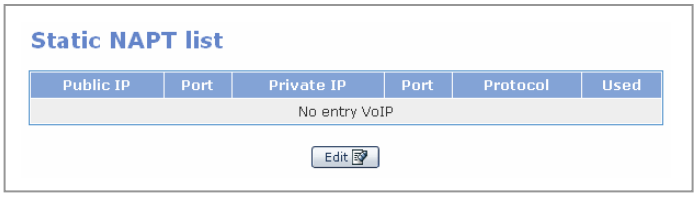
- Public IP: Public IP of the firewall
- Internal IP: Private IP of the internal server connected to the firewall
- Port: Port No. of the service (e.g., Port of the telnet server)
- Protocol: Select a protocol from all/tcp/udp.

NOTE

Specifying a Range of Port

Use the Static NAPT menu if a range of port needs to be specified.

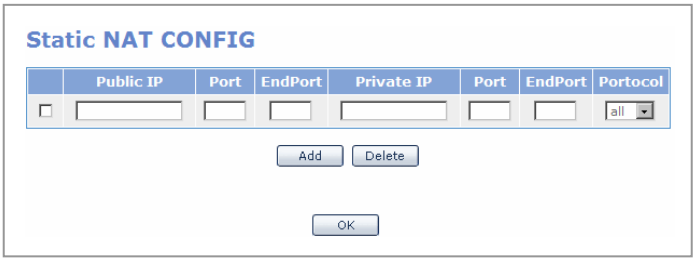
Static NAPT



The ‘Static NAPT list’ window displays the settings of the [Static NAPT] menu.

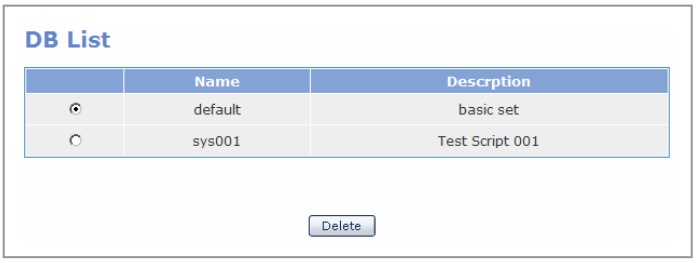
Also, this window displays the ‘VoIP NAPT’ setting in the DSMI menu as well as the user setting of the ‘Static NAPT’ menu.

Click the [Edit] button to switch to a window where the user can enter the settings of Static NAPT.



Network DB List

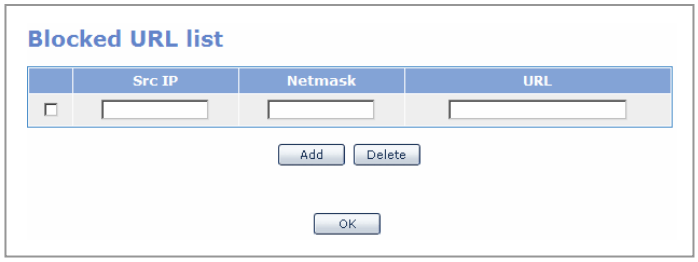
The [DB List] menu is used to delete the settings file saved in the [Management] → [Config] menu.



Filtering Service

The [Filtering Service] menu is used to block the internal local area network users from accessing to a specific URL or IP locations on the Internet.

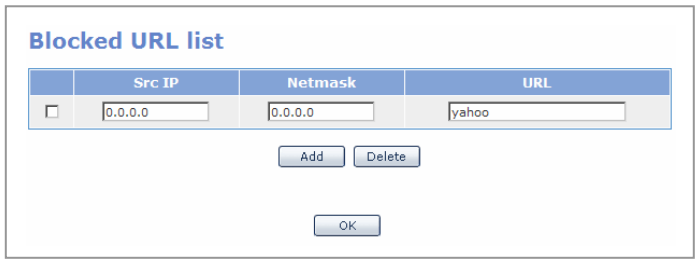
URL Filtering



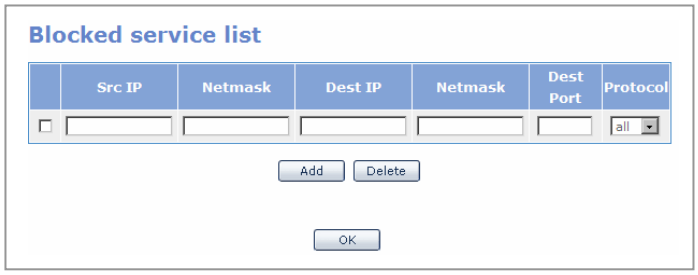
The [URL Filtering] menu is used to block access to a specific URL from an internal host or network.

- SrcIP: An internal host or network where filtering will be performed. Enter the IP address to filter URLs from each host and the network address to filter URLs from each network.
- Netmask: Set Netmask to '255.255.255.255' in order to filter URLs from each host. Enter the subnet of the network to filter URLs from each network.
- URL: Name of a site (Domain) to be blocked

The figure below illustrates an example of blocking access to 'yahoo' by all internal users. Enter values as shown in the figure below and click the [OK] button to complete the settings.



IP Filtering



The [IP Filtering] menu is used to block access to a specific service of an external IP by internal users. Enter the IP address and netmask in the 'Src IP' and 'Netmask' fields, and information on a specific service of the external network to which access will be blocked in the 'Dest IP', 'Netmask', 'Dest Port', and 'Protocol' fields.

If the user enters the network IP and subnet in the Src IP and Netmask fields, the user can enable filtering of an entire network.

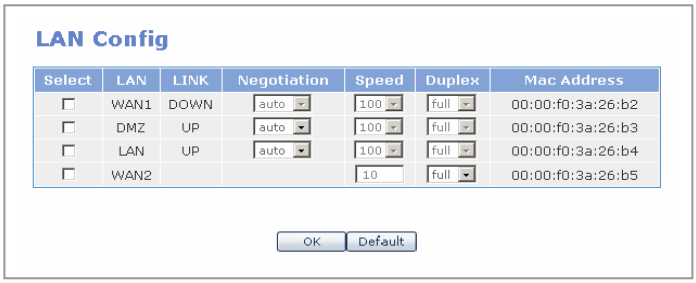
Click the [Add] button, and enter values as shown in the above figure. Click the [OK] button. Then, any terminals cannot access Ports 80 and 22 whose destination address is '211.17.127.70'.

LAN Config

The [LAN Config] menu sets the negotiation, speed, and transfer system for each port.

Select the checkbox of the port to set and click [OK].

Click [Default] to reset to the default value.



Item	Description
Negotiation	- auto: Controls speed through negotiation. - force: Controls speed through enforcement. Set this item to 'force' when setting the Duplex item to 'full'.
Speed (Mbps)	Transfer rate of port
Duplex	- full: Bi-directional service (full-duplex system) - half: Unidirectional service (half-duplex system) Setting for the WAN2 10 M interface depends on the counterpart modem.

Switch Menus

Select [Switch] to display the submenus of Switch on the upper left section of the window.

Menu	Submenu	Description
Port	Config	Sets the switch port environment.
	Statistics	Displays the link status, speed, transmission system, and statistics of the switch port.
VLAN	Config	Configures Virtual LAN(VLAN).
	Port VID	Sets processing method for untagged packets when VLAN mode is set to 'Tag-based VLAN'.
MAC	Static Address	Saves MAC address to the static address table of the switch.
	Dynamic Address	Retrieves the dynamic address table or deletes a MAC address.
	Filter Address	Enters the MAC address to block the frame data with the MAC address information identical with the entered value from the switch.
STP	Config	Prevents broadcast storming due to the switch loop-back using the STP function.
	Port Config	Retrieve the STP status of each port. Enters the new Path Cost and Port Priority values for each port.
IGMP Config	-	Efficiently processes multicast packets through IGMP snooping.

© SAMSUNG Telecommunications America, L.P.

(Continued)

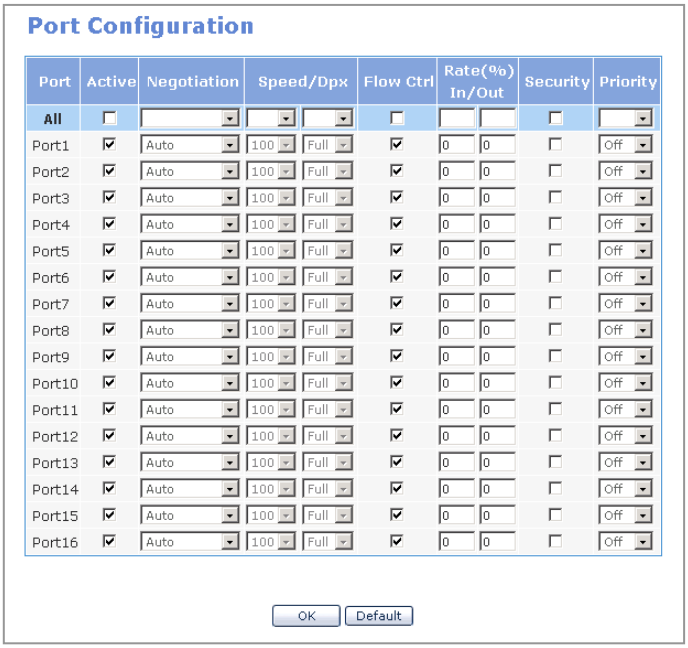
Menu	Submenu	Description
QoS Config	-	Processes Quality of Service by sequentially assigning priority to packets entering the switch or by enforcing priority on a specific port.
MISC Config	-	Sets mirroring and other switching functions.
Save Config	-	Saves setting to flash disk or initializes all setting values.

Port

The [Port] menu is used for setting port related functions and retrieving information on a port.

Config

Select [Port] → [Config] to set the environment of a switch port.

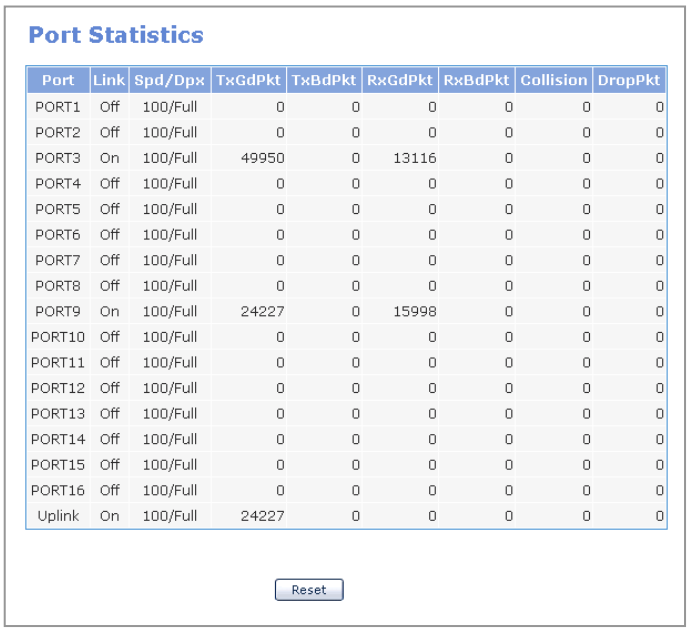


Item	Description
Port	Manage 16 10/100MB Ethernet switch ports Select All to process all ports simultaneously.
Active	Use to activate and de-active the port.
Negotiation	- Auto: Controls speed through negotiation. - Force: Controls speed through enforcement. Set this item to 'force' when Full Duplex is selected for Speed. - Nway Force
Speed/Dpx	- Speed: By default the speed is set according to the value set in 'Path Cost' of the [Switch] → [STP] → [Port Config] menu. 10 Mb/s when 'Path Cost' is set to '100', and 100 Mb/s when set to '19'. If the port has been set to auto-negotiation mode, the local ports will automatically negotiate the port speed. - Dpx(Duplex): Full: Set the port to full duplex to send and receive data packets at the same time for bi-directional service. Half: Set the port to half-duplex to either send or receive only for the unidirectional service. If the port has been set to auto-negotiation mode, the local ports will automatically negotiate the duplex mode.
Flow Ctl	Enable or disable the flow control function. Flow control is performed according to the value set for Rate (%) In/Out (incoming rate/outgoing rate). Limiting the rate at which a port can receive or send traffic is used to ease congestion on bottlenecks in the network and provide simple prioritization when the network is busy.
Rate (%) In/Out	Flow can be controlled by setting the incoming and outgoing rate in percentage for each port. The unit is the ratio against port speed, and should be set to '0' when flow control item is not checked.
Security	Enable or disable the MAC address security check function. This Security check function allows the system to prevent any unauthorized terminal to be connected to the port based on the MAC address. - Disable: System default value, system will not perform MAC address check function. - Enable: If the switch port where 'Security' is checked, only the terminal with the MAC address registered under [Switch] -> [MAC] -> [Static Address] could be connected. Thus, the unauthorized terminal whose MAC address not entered in the Static MAC address connecting to the switch will be block.
Priority	Set the priority of each port to 'Off', 'High' or 'Low'. Traffic prioritization allows high priority data, such as time-sensitive and system-critical data to be transferred without being delayed by lower priority data. This field is only valid if the QoS Mode setting under [Switch] → [QoS Config] → [QoS Configuration] menu is set to <All High before Low> or <Weighted Round Robin>. - Off: no priority is set - 'Low' or 'High': The priority is set to 'Low' or 'High', regardless of the QoS bit settings of the packet received by the port.

© SAMSUNG Telecommunications America, L.P.

Statistics

The [Port] → [Statistics] menu provides a summary of the current switch's status, including link status, speed, transmission system, and statistics. The numbers show the accumulated values for the period from the system boot up to date. The window is automatically updated every five seconds. Click the [Reset] button to initialize all values to '0'.



Port Statistics

Port	Link	Spd/Dpx	TxGdPkt	TxBdPkt	RxGdPkt	RxBdPkt	Collision	DropPkt
PORT1	Off	100/Full	0	0	0	0	0	0
PORT2	Off	100/Full	0	0	0	0	0	0
PORT3	On	100/Full	49950	0	13116	0	0	0
PORT4	Off	100/Full	0	0	0	0	0	0
PORT5	Off	100/Full	0	0	0	0	0	0
PORT6	Off	100/Full	0	0	0	0	0	0
PORT7	Off	100/Full	0	0	0	0	0	0
PORT8	Off	100/Full	0	0	0	0	0	0
PORT9	On	100/Full	24227	0	15998	0	0	0
PORT10	Off	100/Full	0	0	0	0	0	0
PORT11	Off	100/Full	0	0	0	0	0	0
PORT12	Off	100/Full	0	0	0	0	0	0
PORT13	Off	100/Full	0	0	0	0	0	0
PORT14	Off	100/Full	0	0	0	0	0	0
PORT15	Off	100/Full	0	0	0	0	0	0
PORT16	Off	100/Full	0	0	0	0	0	0
Uplink	On	100/Full	24227	0	0	0	0	0

Reset

- TxGdPkt: The number of packets which are successfully sent to the port
- TxBdPkt: The number of packets which are switched, but not successfully transmitted to the port.
- RxGdPkt: The number of packets which are successfully received by the port.
- RxBdPkt: The number of packets which are successfully received by the port, but not successfully switched.
- Collision: The number of collision occurred between packets received from the port and the switched packets
- DropPkt: The number of packets which are not switched to the port, but are dumped in the buffer.

© SAMSUNG Telecommunications America, L.P.

VLAN

The [VLAN] menu is used for configuring Virtual LAN(VLAN).

A Virtual LAN (VLAN) is a logical network grouping that provide separation of broadcast domains and functional work area to improve performance. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network device to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

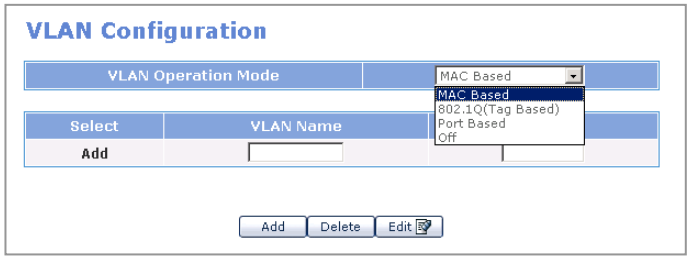
OfficeServ 7200 managed switch supports the following VLAN configurations:

- MAC Based
- 802.1Q Tag Based
- Port Based

In the default configuration, VLAN support is disabled.

Config

Select [VLAN] → [Config] to display the VLAN configuration window.



Select a VLAN mode from the 'VLAN Operation Mode' and click the [OK] button. Then, enter a VLAN name and ID and click the [Add] button to add the VLAN.
Check a VLAN and click the [Delete] button to delete the VLAN.

VLAN configuration is determined according to the three VLAN modes below:

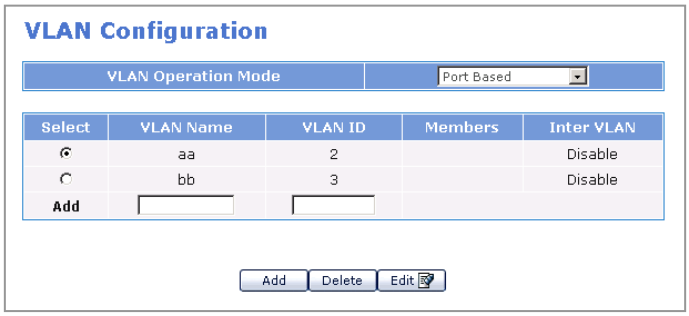
- Port Based VLAN
- Tag Based VLAN(802.1 Q)
- MAC Based VLAN

Port Based VLAN

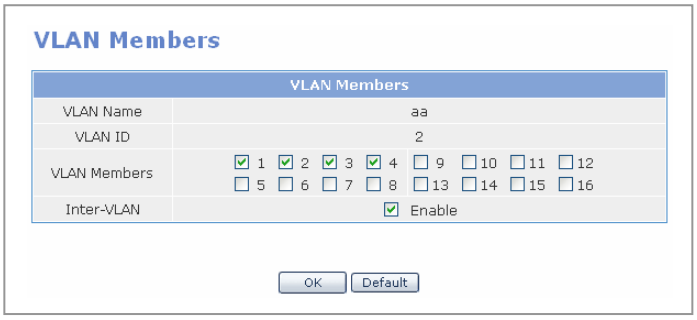
This option is used to configure VLAN on port basis. Packets can only be broadcast among members of the same VLAN group. A single port can be assigned to multiple VLANs. All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

© SAMSUNG Telecommunications America, L.P.

Select ‘Port Based’ as the VLAN Operation Mode from the <VLAN Configuration> window.



Select a VLAN and click the [Edit] button to display the window shown below. Select the target port at VLAN Members and click the [Save] button.



Inter-VLAN Communication

To perform communication between VLANs, enable the Inter-VLAN service. If the devices placed in a VLAN need to communicate with devices in a different VLAN, a shared port with connections to both VLANs needs to be present. OfficeServ 7200 WIM router will provide the the inter VLAN communication as it has an IP interface on each VLAN.

Thus if the WIM and LIM are connected through the backbone, the inter-VLAN communication will use that physical port as the shared port.

On the other hand, if the jumper pin of the WIM board is set toward the front side of the board, the port on the LIM that is used to connect with the LAN port of the WIM board, should be set as a VLAN member.

Tag Based VLAN (802.1 Q)

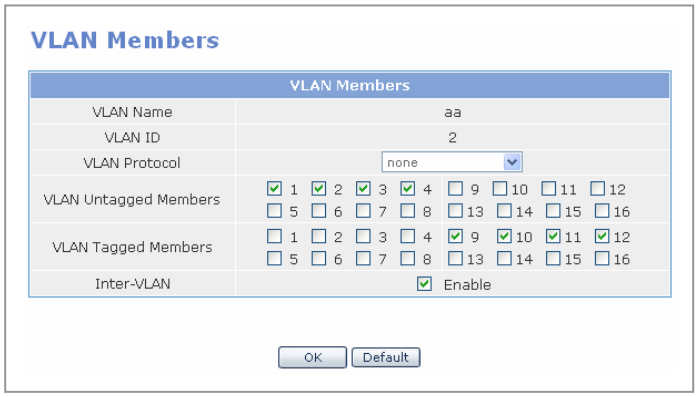
Tag-based VLAN is an IEEE 802.1Q specification standard. IEEE 802.1Q VLAN uses a technique to insert a ‘tag’ into the Ethernet Frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers. Enable 802.1Q VLAN, all ports on the switch belong to default VID of 1. OfficeServ 7200 supports up to 256 tag-based VLAN groups.

Packets not including tags are delivered to a single VLAN and its VLAN ID is defined in the menu [VLAN] -> [Port VID].

Tag Based VLAN is composed of tagged members and untagged members. This determines whether or not the system will remove (untag) tags before sending traffic out of each port.

Select 'Tag Based' as the VLAN Operation Mode from the <VLAN Configuration> window

1. Type a name for the new VLAN.
2. Type a VID (between
3. Click the [Edit] button to display the window shown below.
4. Select the protocol type. OS 7200 support 802.1v with the implementation of Port-and-Protocol- based VLAN classification. User can combine the field 'Protocol VLAN' and the field of the port member to form a new VLAN group.
5. Select the ports to set the outgoing frames for VLAN-Tagged frame or no.
    - VLAN Untagged Members: outgoing frame without VLAN-Tagged
    - VLAN Tagged Members: outgoing frames with VLAN-Tagged.
6. Click the [Save].



- VLAN Untagged Members: If one of ports(1~16) is determined for switching and transmission, select a port for delivering the Ethernet frame from which the tag information is deleted.
- VLAN Tagged Members: If one of ports(1~16) is determined for switching and transmission, select a port for storing and sending the tag information. Connect the IEEE 802.1Q-supported terminal to the selected port.

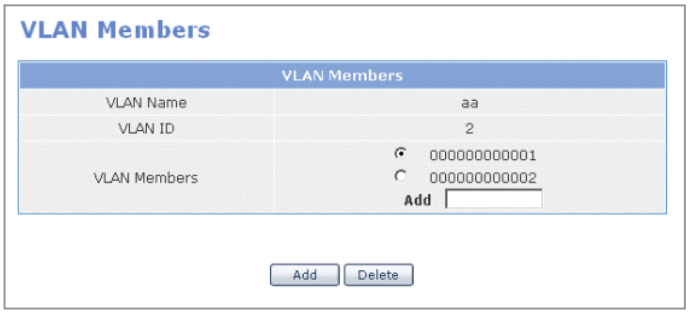
© SAMSUNG Telecommunications America, L.P.

MAC Based VLAN

Membership in MAC Based VLAN is based on assigning the MAC address of a device to a VLAN. VLAN is configured without information on port and the number of a VLAN member may change. The advantage of MAC based VLAN is that even if users relocate, they remain on the same VLAN as long as they stay connected to the same switch. Up to 1024 MAC members can be saved either in a single VLAN or in multiple VLANs.

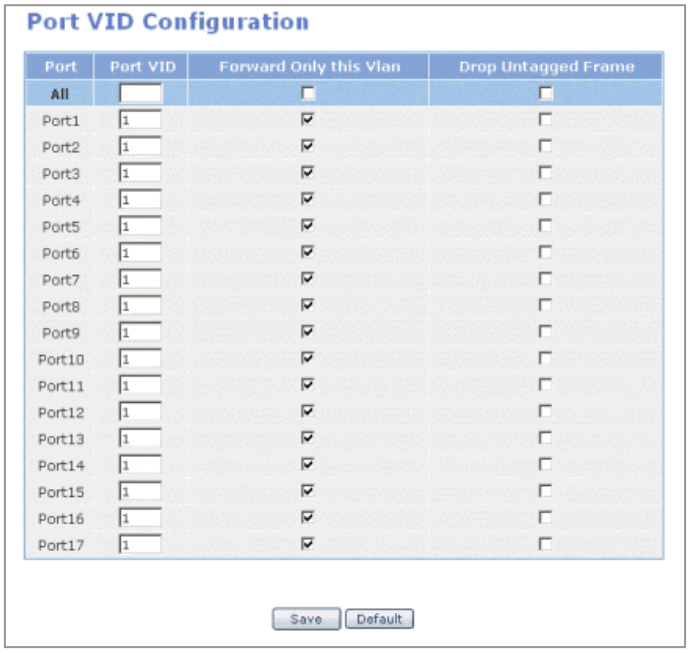
Since a MAC Based VLAN does not basically contain port information, the port serves as a VLAN member by receiving Address Resolution Protocol(ARP). Thus, the ARP packet must be transmitted to the switch to enable members of a VLAN to exchange packets.

Select 'MAC Based VLAN' as the VLAN Operation Mode from the <VLAN Configuration> window and click the target VLAN, and click the [Edit] button to display the window shown below. Enter the MAC address of a member into the 'Add' field and click the [Add] button to add the member or click the [Delete] button to delete the member.



Port VID

If the VLAN mode is 'Tag-based VLAN', the Port VID is set at the [VLAN] → [Port VID] menu to determine the processing system for untagged packets. This feature is useful for accommodating devices that you want to participate in the VLAN but they don't support tagging. OS 7200 switch allows user to set one PVID for each port, the range is 1 to 255 with default PVID of 1. The PVID must be the same as the VLAN ID that port belongs to in the VLAN group, or the untagged traffic will be dropped.



Item	Description
Port VID	VLAN ID for untagged packets, value between 1 and 255. Default Port VID is 1. If the Untagged packet is received by the port, the packet is switched to VLAN identical to Port VID.
Forward Only this Vlan	Selected: forward only the packet with VID matching this port's configured VID. Not selected: the packet is retransmitted according to the received Tag information.
Drop Untagged Frame	Selected: drop the untagged packet. Not selected: retransmit untagged packets only to VLAN corresponding to the designated Port VID.

NOTE

VID Setting

In a mode where the 802.1Q VLAN is set, enter the 'VLAN ID' value when entering settings in the 'Static Address', 'Filter Address' menu. If the value is not entered, '0' is set.

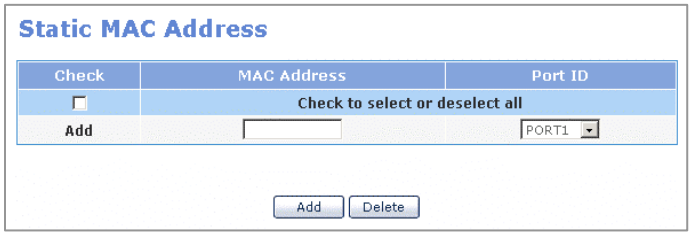
© SAMSUNG Telecommunications America, L.P.

MAC

The [MAC] menu is used for retrieving the address table of the switch or for setting Filtering MAC.

Static Address

Select [MAC] → [Static Address] to save a MAC address to the address table of a switch regardless of whether the device and switch is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again.



Enter the MAC address and port No., and click the [Add] button.
Select a MAC address and click the [Delete] button to delete the address.
If Security of the port is set in the [Port] → [Config] menu, the learning for the source MAC address is not performed. In this case, since the Static MAC address set in the port is allowed to access the port, it is possible to set the security function using it.

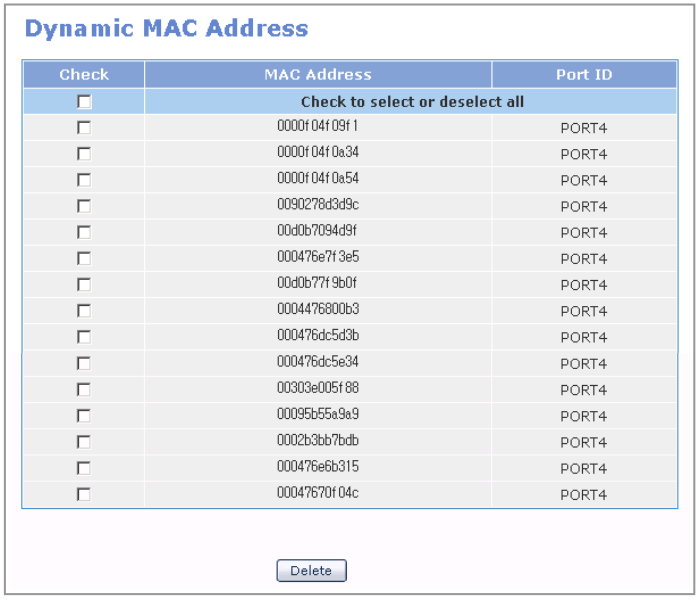
NOTE

Number of Static MAC Address Input

Regardless of port, you can enter 50 Static MAC Addresses in total.

Dynamic Address

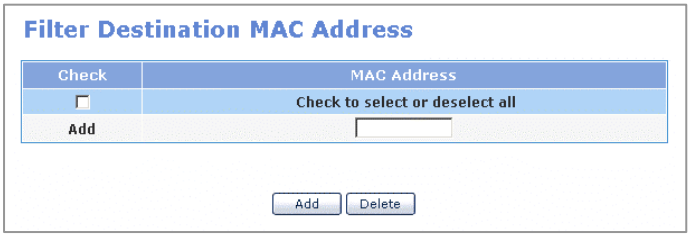
Select [MAC] → [Dynamic Address] to retrieve the current MAC adress that the switch has learned.



Select a MAC address and click the [Delete] button to delete the address.

Filter Address

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. Select the [Filter Address] menu and enter a MAC address to block the corresponding packet from the switch. The MAC address is the destination address of a packet entering the switch port.



Enter the MAC address and port No. and click the [Add] button.
Select a MAC address and click the [Delete] button to delete the address.

© SAMSUNG Telecommunications America, L.P.

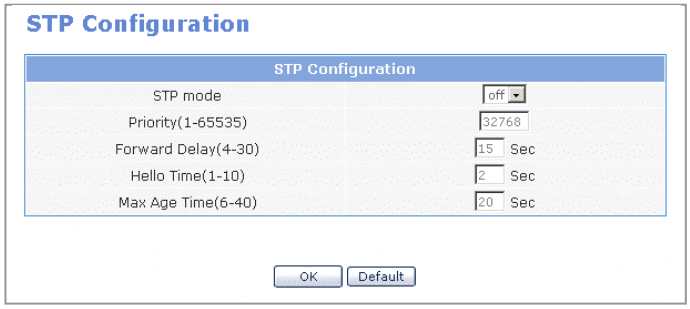
STP

The [STP] menu is used to set the Spanning Tree Protocol (STP) function or to retrieve STP status.
The Spanning Tree Protocol is a standardized method (IEEE 802.1D) to provide path redundancy while preventing endless loops of traffic in switched network. Loops occur when there are alternate routes between hosts.

- To establish path redundancy, STP creates a tree that spans all of the switches in a network, forcing redundant paths into a standby state.
- STP allows only one active path at a time between any two network devices but establishes the redundant links as a backup if the initial link should fails.
- If STP costs change, or if one network segment in the STP becomes unreachable, STP reconfigures the spanning tree topology and re-establishes the link by activating the standby path.

Config

Select [STP] → [Config] to set STP and to prevent switch loop-back.

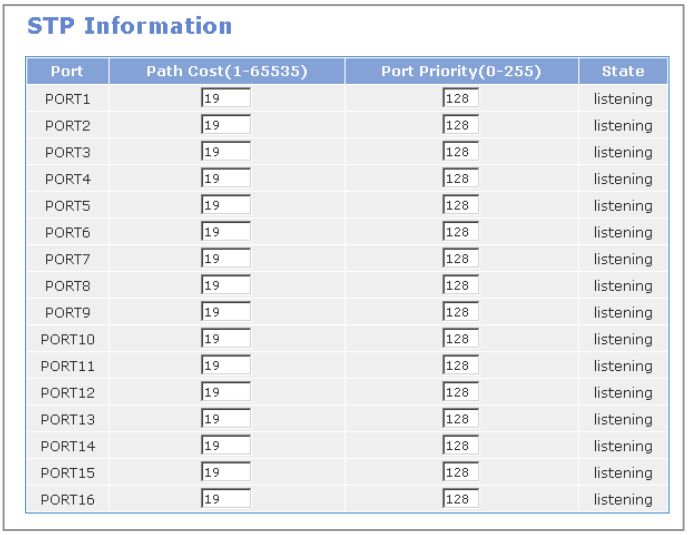


Item	Description
STP Mode	Disable or enable STP. STP is disabled by default.
Priority	Set priority for deactivating ports in case switch loop-back occurs. The priority is used to identify the root bridge. Bridge with the lowest value has the highest priority and is selected as the root. Enter a number 1 through 65535.
Forward Delay	Forward delay time, set number of seconds a port waits before changing from its STP configuration messages. Enter a number 4 through 30.
Hello Time	Set the transmission interval for STP set messages. Enter a number 1 through 10.
Max Age Time	Set the number of second bridge waits without receiving STP configuration before attempting a reconfiguration. Enter a number 6 through 40.

© SAMSUNG Telecommunications America, L.P.

Port Config

Select [STP] → [Port Config] to set or retrieve STP status.



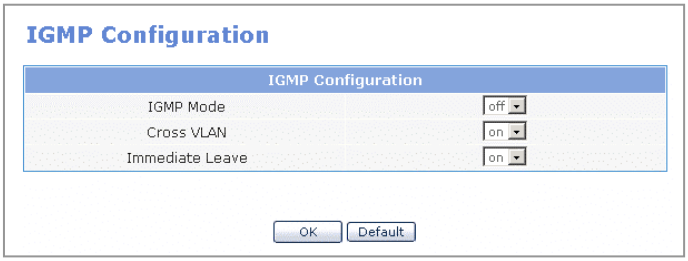
Item	Description
Port	16 switch ports are equipped in all. Select All to process all ports simultaneously.
Path Cost	Set the path cost of the port that switch uses to determine which port are the forwarding ports. The port with the lowest number will be selected as the forwarding port. Set to '100' for 10 Mb/s, and to '19' for 100 Mb/s. The 'Speed' value of the 'Speed/Dpx' item at the [Switch] → [Port] → [Config] menu is automatically set according to the setting of this item.
Port Priority	Set priority for deactivating ports in case switch loop-back occurs. The default setting is 128. Note: The lowest number has the highest priority.
State	Indicates the status of each port. - blocking: If a loop occurs on the switch, the corresponding port is blocked and data is no longer sent to the port. - listening: The port is learning the path to the Root Bridge, and can transmit/receive BPDU (Bridge Protocol Data Units, frames which carry the spanning tree protocol information). However, the port cannot send data nor update the MAC address table. This status continues for the time length set in the 'Forward Delay' item of the <STP Configuration> window. - learning: Similar to 'listening', but can exchange BPDU and update the MAC address table. However, data cannot be sent. This status continues for the time length set in the 'Forward Delay' item of the <STP Configuration> window. - forwarding: Normal communication is enabled.

© SAMSUNG Telecommunications America, L.P.

IGMP Config

The [IGMP Config] menu is used to efficiently process multicast packets through Internet Group Management Protocol(IGMP) snooping. IGMP is the standard for IP multicasting in the Internet. It is used to establish host membership in particular multicast groups on a single network. IGMP allows a host to inform its local router, using Host Membership Reports, which it wants to receive messages addressed to a specific multicast group.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP Snooping generates no additional network traffic, allowing a significantly reduced multicast traffic passing through the switch.

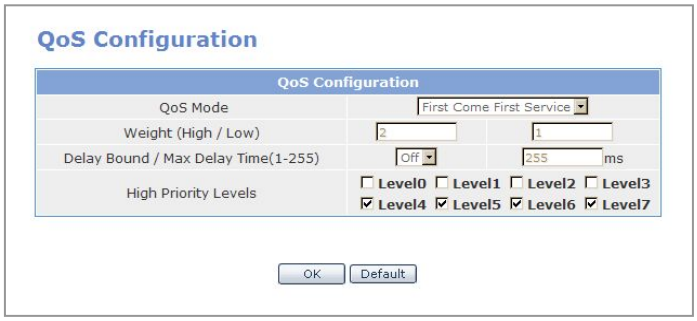


Item	Description
IGMP Mode	Set whether to perform multicasting through IGMP snooping. If the IGMP snooping is not used, the received multicasting packet is broadcasted. By default, IGMP is disabled.
Cross VLAN	If this item is set, it is possible to transmit a packet between different VLANs when the multicasting packet reaches the switch.
Immediate Leave	Set this item to delete a member from the multicast table upon receiving the IGMPv2 Leave message. This also enables information to be quickly applied to the multicast table when the hosts are directly connected to the switch ports.

© SAMSUNG Telecommunications America, L.P.

QoS Config

The [QoS Config] menu is used for processing QoS by sequentially assigning priority to packets entering the switch or by enforcing priority on a specific port. OfficeServ 7200 managed switch provides Layer 2 QoS functionality to better prioritize and manage packets.



Item	Description
QoS Mode	Select the QoS mode. - First Come First Service: The sequence of packets sent is depending on arrive orders. (QoS is not used.) - All High before Low: Packets with higher priority are sent ahead of those with lower priority. Packets with a low priority are not transmitted until packets with a high priority are transmitted. - Weighted Round Robin: Packets with a high priority and packets with a low priority are transmitted according to the fixed weight. For example, setting High weight to '5' and Low weight to '2' will send five higher priority packets before sending two lower priority packets.
Weight	If the user wants to use a 'Weighted Round Robin' method, set the ratio of high weight to low weight.
Delay Bound/ Max Delay Time	Limit the low priority packets queuing time in switch when the QoS mode is 'All High before Low' or 'Weighted Round Robin'. The unit of 'Max Delay Time' is ms (1/1000 sec) and the initial value is 255 ms. If the low priority packet stays in switch exceed Max Delay Time, the packet will be sent. The valid range is 1 to 255ms.
High Priority Levels	Assign the CoS values for the High Priority Levels queue. OfficeServ 7200 LIM switch supports 2 output queues, High and Low. Each queue can be assigned using 802.1p CoS values. 802.1p CoS operates at Layer 2 of the OSI model, and values range from 0 to 7 with 0 being lowest priority. CoS values of level 4 -7 are assigned to High Priority Queue by default.

© SAMSUNG Telecommunications America, L.P.

MISC Config

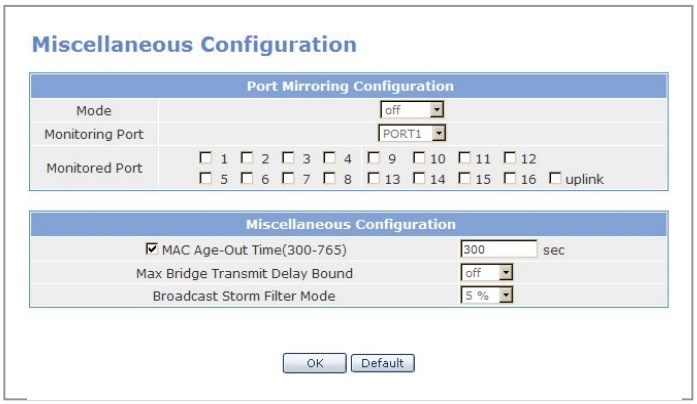
The [MISC Config] menu is used for setting the mirroring function and other switching functions.

Port Mirror

The Port Mirror is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That is all traffic goes in or out of the monitored port will be duplicated into mirror port.

Broadcast Storm Filter

To configure broadcast storm control, enable the broadcast storm filter and set the upper threshold for the individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When the broadcast traffic for a port rises above the threshold, broadcast storm control becomes active. The valid threshold value is 5%, 10%, 15%, 20%, 25%, and off.



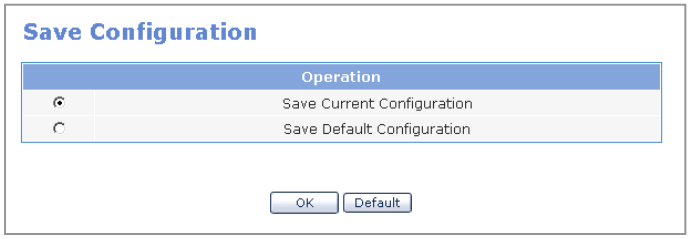
Item	Description
Mode	Set whether to use mirroring. - Off: Do not use mirroring - Tx: Use mirroring for Tx packets - Rx: Use mirroring for Rx packets - Both: Use mirroring for Tx and Rx packets
Monitoring Port	Set the port performing monitoring. Generally, it means the connection port of a PC for monitoring.
Monitored Port	Set the target port of monitoring. All monitor traffic will be copied to mirror port. A maximum of 16 monitor ports can be selected. User can choose which port that they want to monitor in only one mirror mode.

© SAMSUNG Telecommunications America, L.P.

Item	Description
MAC Age-Out Delay Bound	Set the time during which an updated MAC address(Learning) may remain in the address table. Default value is 300 sec. In case of the unmanaged LIM that is not controlled by WIM, if the LAN port is disconnected, the updated MAC address is automatically deleted in 300 seconds. Therefore, the new MAC address is not updated immediately when the LAN port is connected again. In case of the managed LIM(installed into Slot 2) controlled by WIM, if the LAN port is disconnected, the updated MAC address is deleted automatically and immediately. The new MAC address and MAC address table are updated at a fast speed when the LAN port is connected again.
Max Bridge Transmit Delay Bound	Set maximum packet waiting time to Off, 1 sec, 2 sec , or 4 sec.
Broadcast Storm Filter Mode	Set among 5, 10, 15, 20, 25 % of the total buffer size. Broadcast packets exceeding this value are lost.

Save Config

The [Save Config] menu is used to save settings to the flash disk. Since settings are basically saved in RAM, the settings will be lost when system is turned off. The settings are saved in the flash disk to prevent the data from being erased during rebooting.



Item	Description
Save Current Configuration	Saves current setting to flash disk. If the system is rebooted without saving the setting, the setting will be lost and will not be applied to the system.
Save Default Configuration	Changes settings in the flash disk to default values. Default values are applied after system rebooting.

NOTE

Saving or Importing the Switch DB

Click [System] → [DB Config] → [Save/Delete] to save the Switch DB.
Click [System] → [DB Config] → [Import/Export] to import the saved DB. Reset the WIM system to import the DB.

© SAMSUNG Telecommunications America, L.P.

Router Menus

Select the [Router] menu to display the submenus of Router on the upper left section of the window.

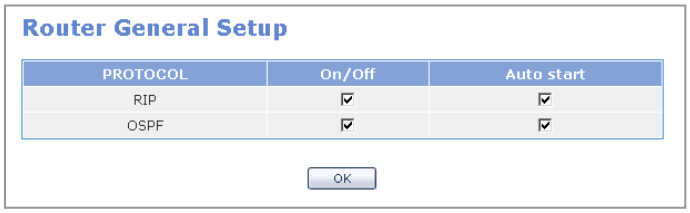
Menu	Submenu	Description
General	Show Route	Displays the routing table of the Data Server.
	Management	Starts or stops RIP and OSPF services, and can set whether to execute the services upon system rebooting.
Config	Static Route	Sets static route.
	RIP config	Sets RIP.
	OSPF config	Sets OSPF.

General

The [General] menu is used for starting or stopping RIP and OSPF services and for retrieving the routing table of the Data Server.

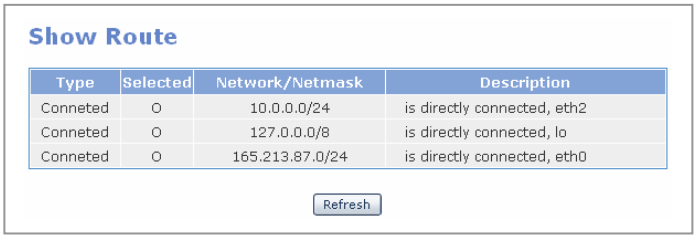
Management

Select [General] → [Management] to start or stop the RIP and OSPF services. Check the 'Auto Start' item to start the service automatically when the system is rebooted.



Show Route

Select [General] → [Show Route] to retrieve the routing table of the Data Server.



Item	Description
Type	- Connected: Network is directly connected to the network interface of the Data Server - RIP: Route data received from other routers through RIP - OSPF: Route data received from other routers through OSPF
Selected	Indicates whether routing is activated
Network/Netmask	Network information on the route
Description	Description on the route

© SAMSUNG Telecommunications America, L.P.

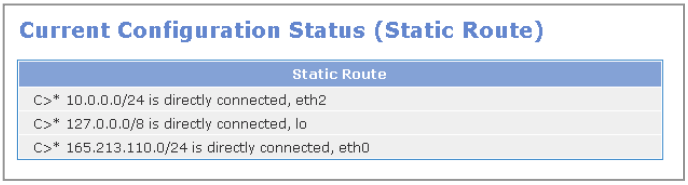
Config

The [Config] menu is used for setting static route, RIP, and OSPF.

Static Route

Select [Config] → [Static Route] to set static route. Set the following items and click the [Save] button:

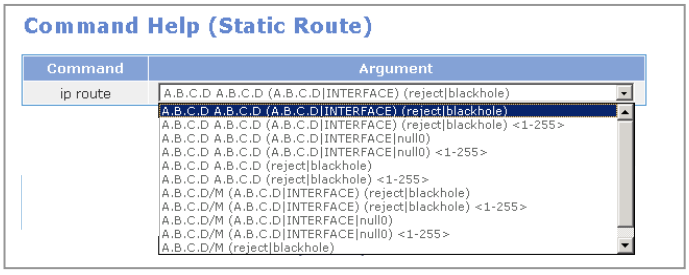
- Current Configuration Status


Current Configuration Status (Static Route)
Static Route
C>* 10.0.0.0/24 is directly connected, eth2
C>* 127.0.0.0/8 is directly connected, lo
C>* 165.213.110.0/24 is directly connected, eth0

This window shows the routing table of the Data Server, which is same as that displayed on the window of the [Router] → [General] → [Show Route] menu. However, the above window displays the route type as follows:

Item	Description
C>*	Network route connected to the network interface of the Data Server
O	Route data received from other routers through OSPF
R	Route data received from other routers through RIP
S	Static route set by administrator

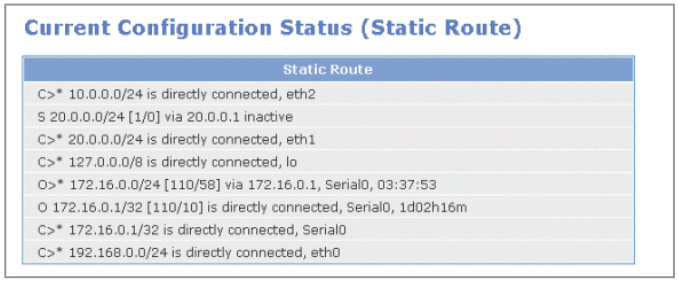
- Input Configuration Command
  Select the argument corresponding to the 'ip route' command.
  Clicking the 'Argument' item displays all arguments corresponding to the command. Select an argument from the list.



© SAMSUNG Telecommunications America, L.P.

- Input Configuration Command
  Select a command as shown above, or directly enter the static route setup command as shown below:

The command execution result is directly applied to the <Current Configuration Status> window of the [Router] → [Config] → [RIP Config] menu. For example, the result of entering the static route command as above is displayed on the <Current Configuration Status> as shown below:


Current Configuration Status (Static Route)
Static Route
C>* 10.0.0.0/24 is directly connected, eth2
S 20.0.0.0/24 [1/0] via 20.0.0.1 inactive
C>* 20.0.0.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.0.0/24 [110/58] via 172.16.0.1, Serial0, 03:37:53
O 172.16.0.1/32 [110/10] is directly connected, Serial0, 1d02h16m
C>* 172.16.0.1/32 is directly connected, Serial0
C>* 192.168.0.0/24 is directly connected, eth0

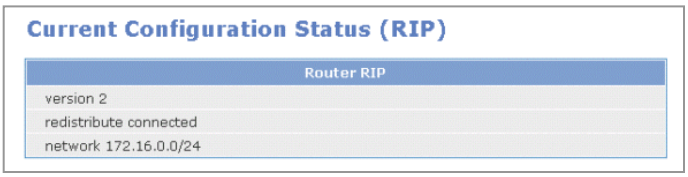
Deleting Static Route

To delete the set Static Route information, attach 'no' before ip route. In other words, if you enter 'no ip route 20.0.0.0/24 20.0.0.1' , the set Static Route information is deleted.

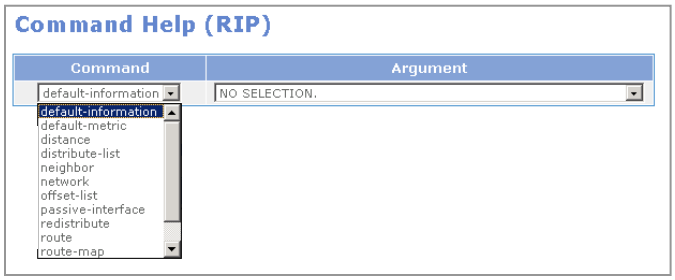
RIP Config

Select [Config] → [RIP Config] to set RIP. Set the following items and click the [Save] button:

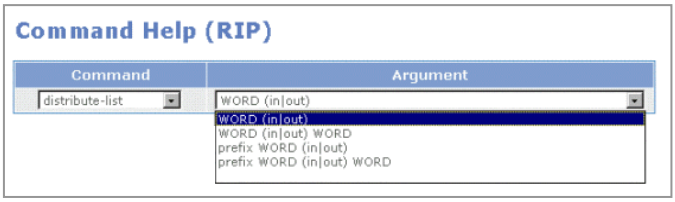
- Current Configuration Status
  This item displays the current RIP status.
  The status is updated when the RIP command entered into the <Input Configuration Command> window of the [Router] → [Config] → [Static Route] menu is executed.



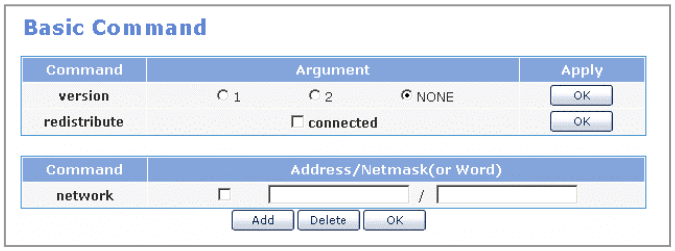
- Command Help
  Select a RIP command from the ‘Command’ item and select an argument for the command from the ‘Argument’ item.



For example, the arguments for the ‘distribute-list’ command are as follows:



- Basic Command
  After entering the items, click the [OK] button to display the applied value on the <Current Configuration Status> window.



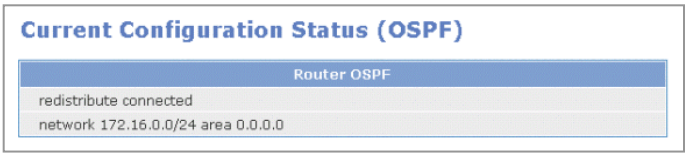
- Input Configuration Command
  Select a command, as if selecting one from the <Command Help(RIP)> window, or directly enter a RIP command and click the [OK] button.

© SAMSUNG Telecommunications America, L.P.

OSPF Config

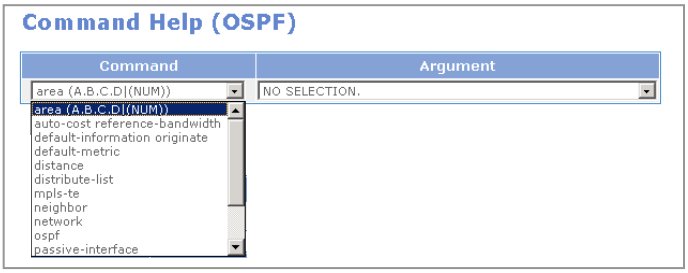
Select [Config] → [OSPF Config] to set OSPF. Set the following items and click the [Save] button.

- Current Configuration Status
  This item displays the current OSPF status. The status is updated when the OSPF command entered into the <Input Configuration Command> window of the [Router] → [Config] → [Static Route] menu is executed.

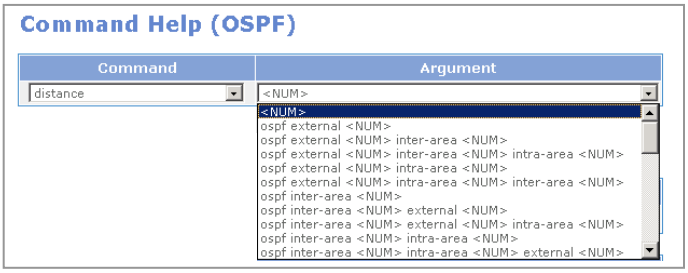


If set as 'area 0.0.0.0' as shown above, the information on the route directly connected to the network interface of the Data Server is delivered through 'network 172.16.0.0'.

- Command Help
  Select an OSPF command from the 'Command' item and select an argument for the command from the 'Argument' item.

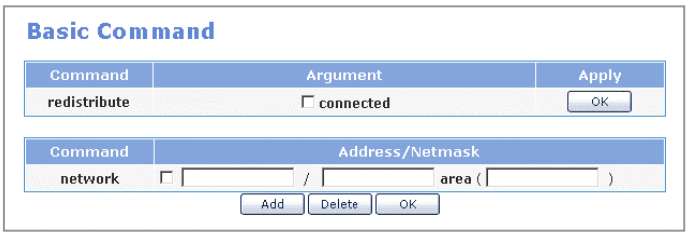


For example, the arguments for the 'distance' command are as follows:



© SAMSUNG Telecommunications America, L.P.

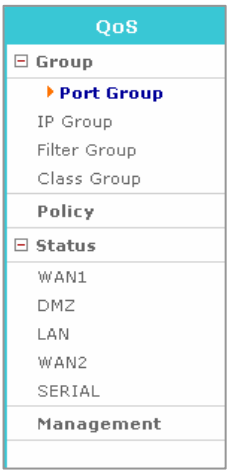
- Basic Command
  After entering the items, click the [OK] button to display the applied value on the <Current Configuration Status> window.



- Input Configuration Command
  Select a command, as if selecting one from the <Command Help(RIP)> window, or directly enter an OSPF command and click the [OK] button.

QoS Menus

Select the [QoS] menu to display the submenus of QoS on the upper left section of the window.



Menu	Submenu	Description
Group	Port Group	Retrieves, sets, edits, or deletes a port group
	IP Group	Retrieves, sets, edits, or deletes an IP group
	Filter Group	Retrieves, sets, edits, or deletes a filter group
	Class Group	Retrieves, sets, edits, or deletes a class group
Policy	-	Sets a class for a port
Status	-	Displays QoS class and filter data of a port in a tree structure
Management	-	Starts or stops the execution of a QoS and can set whether to automatically execute the QoS when the system is rebooted

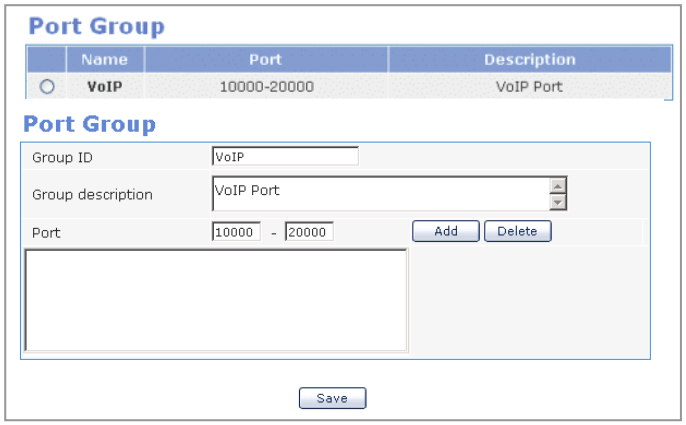
© SAMSUNG Telecommunications America, L.P.

Group

The [Group] menu is used to retrieve, set, edit, or delete a port group, an IP group, a filter group, or a class group.

Port Group

Select [Port Group] to retrieve, set, edit, or delete a port group.



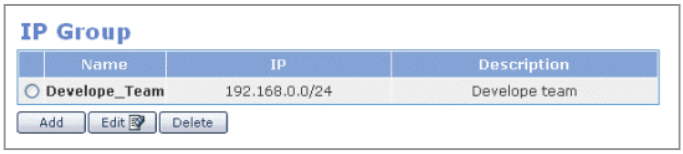
Click the [Add] button in the above window to display a window from which a port group can be set. Enter the group ID, group description, and port number, click the [Add] button, and click the [Save] button.

Item	Description
Group ID	Name of the port group - Should include both letters and numbers - Group ID shall start only with letters, not numbers - No blanks should be left in between characters
Group description	Description on the port group
Port	Range of ports Enter '0' to set all ports

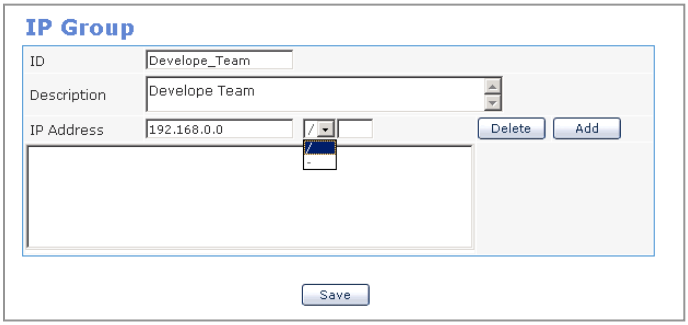
© SAMSUNG Telecommunications America, L.P.

IP Group

Select [IP Group] to retrieve, set, edit, or delete an IP group.



Click the [Add] button in the above window to display a window from which an IP group can be set. Enter the group ID, group description, and port number, click the [Add] button, and click the [Save] button.

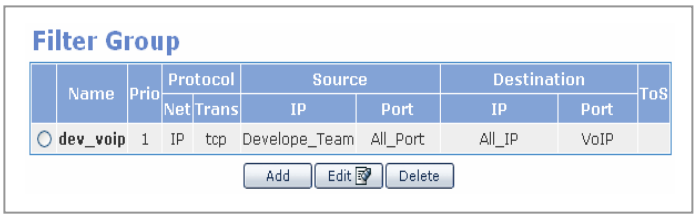


Item	Description
ID	Name of the IP group - Should include both letters and numbers. - Group ID shall start only with letters, not numbers. - No blanks should be left in between characters.
Group description	Description on the IP group
IP Address	IP address /: Used for entering subnet -: Used for entering the range of IPs Enter '0.0.0.0/0' to set all ports.

© SAMSUNG Telecommunications America, L.P.

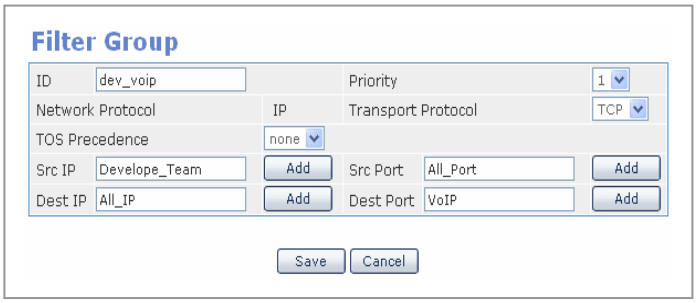
Filter Group

Select [Filter Group] to retrieve, set, edit, or delete a filter group.



If 'dev_voip' is registered as the filter group as shown above, the filtering rule is as follows: 'Source' and 'Destination' are set in the [Port Group] menu and [IP Group] menu. All TCP packet traffics of which the internal IP is Develop_Team(192.168.0.0/24) and the connection port is VoIP(10000~20000) are filtered with a priority of '1'. The filter is then associated with the class group set at the [QoS] → [Group] → [Class Group] menu.

Click the [Add] button in the above window to display a window from which a filter group can be set. Set the items and click the [Save] button. Clicking the [Add] button displays a list of port groups and IP groups. Select the IP and port from the list.



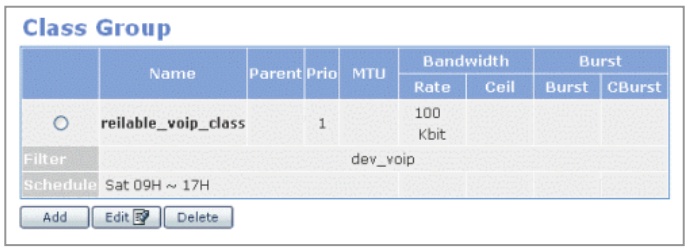
Setting a filter means setting a rule for filtering the values in the packet header. Values set at the [QoS] → [Group] → [Port Group] menu and the [IP Group] menu is used, and protocols and TOS fields can also be filtered. In addition, priorities can be set for the filters to apply the filtering rules according to the priority.

The 'Src IP', 'Src Port' and 'Dest IP', 'Dest Port' are mandatory items and must be entered. If these items are not entered, an error message will appear.

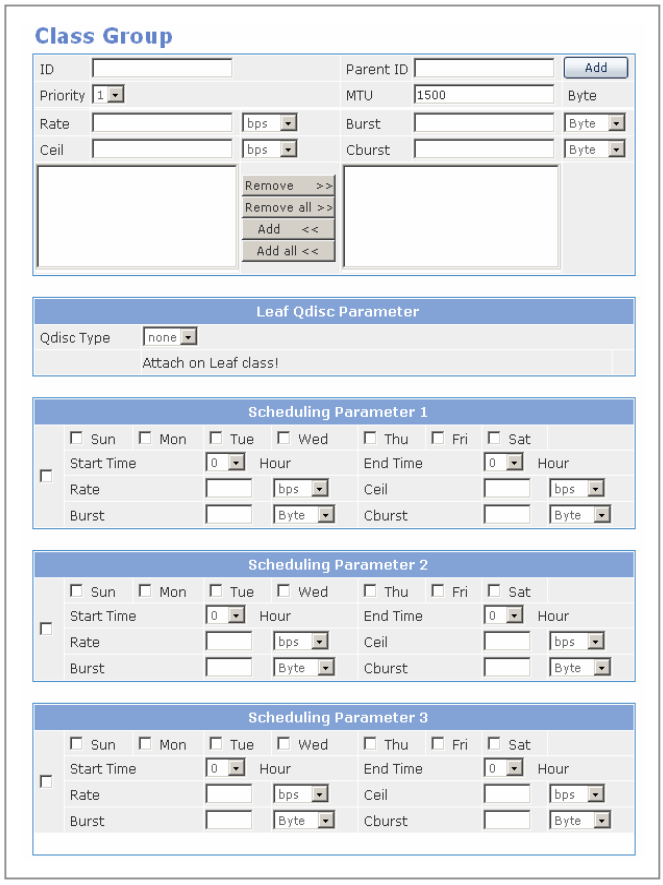
© SAMSUNG Telecommunications America, L.P.

Class Group

Select [Class Group] to retrieve, set, edit, or delete a class group. A class includes information on the defined filtering rule and the bandwidth that should be assigned to the filtered traffic.



Click the [Add] button in the <Class Group> window to display a window from which a class group can be set. Set the items and click the [Save] button.



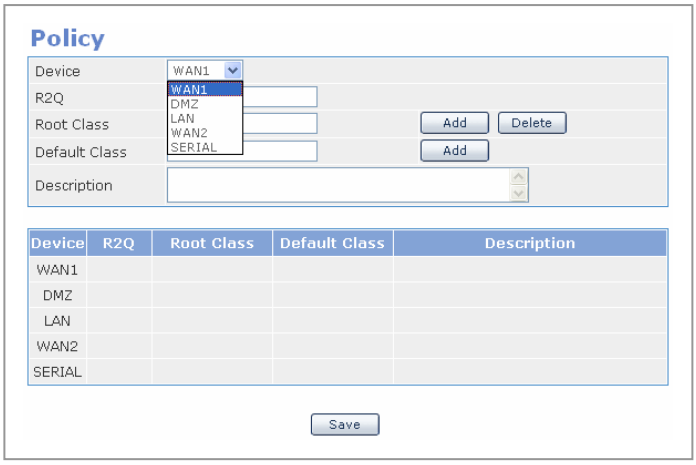
© SAMSUNG Telecommunications America, L.P.

Item	Description
Parent ID	Due to the hierarchical characteristic of QoS, classes are classified into the root class(highest level class) and the leaf class(lowest level class) and into the parent class and the child class. If the target class is a child class of another class, set the parent class in the Parent ID item. Do not set the Parent ID if the target class is the root class(highest level class physically connected to the device) or the default class(class including the bandwidth for traffics that do not belong to a filter).
Priority	If several classes compete to occupy leftover bandwidths or if all classes attempt to occupy excess bandwidth, set the priority so that the class with the highest priority occupies the bandwidth first.
MTU	The Maximum Transmit Unit(MTU) represents the maximum amount of packets that can be transmitted at a time. It is recommended that this setting does not exceed the maximum packet size(1504 Byte) of Ethernet. If this item is not entered, the default value, '1500 Byte', will be applied.
Rate	This is the basic bandwidth needed for setting class for an assigned bandwidth.
Ceil	Maximum value of assigned bandwidth.
Burst	Size of data that can be sent by the class.
Cburst	Maximum data size that can be sent at a time.
Filter List	Sets filtering rules for the class.
Leaf Qdisc Parameter	Set a desired Qdisc for the Leaf Qdisc parameter when setting the lowest level class.
Scheduling Parameter 1/2/3	Changes the bandwidth of the class based on day and hour. Up to three scheduling parameter can be set.

© SAMSUNG Telecommunications America, L.P.

Policy

The [Policy] menu is used for setting a class for a port. Enter the following items and click the [Save] button to select a class for a port.

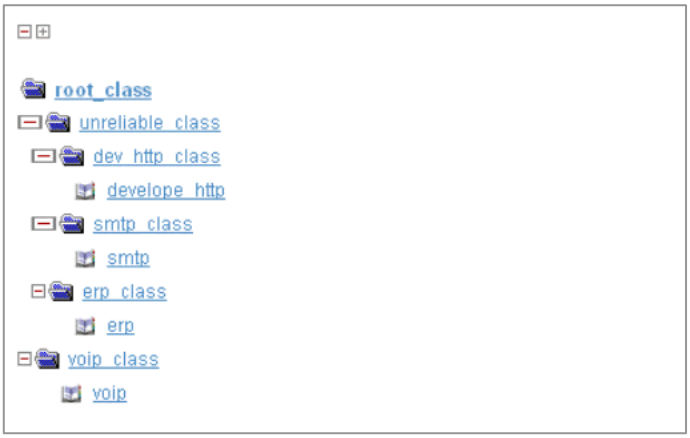


Item	Description
Port	Select a port(select WAN1, DMZ, LAN, WAN2, or SERIAL)
R2Q	R2Q is used as a variable for calculating the amount of Deficit Round Robin(DRR).(Bps/r2q)
Root Class	Class connected to the port. Click the [Add] button and select the class group from the class group list.
Default Class	This class defines the bandwidth for incoming traffics that are not applicable to all filtering rules. Click the [Add] button and select the class group from the class group list.
Description	Input the information on each device.

© SAMSUNG Telecommunications America, L.P.

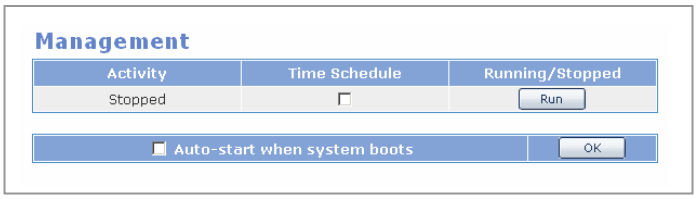
Status

The [Status] menu is used for displaying the class and filters assigned to each port in a tree structure.



Management

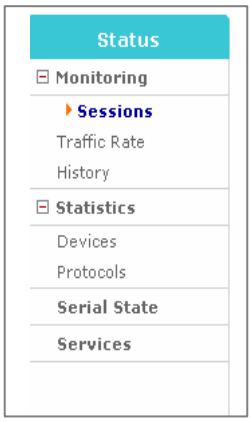
The [Management] menu is used to start or stop the execution of a QoS. Execution of the 'Scheduling Parameter' set at the [QoS] → [Group] → [Class Group] menu can also be started or stopped. Clicking the 'Auto start' item will automatically start the QoS service when the



system is rebooted.

Status Menus

Select [Status] to display the submenus of Status on the upper left section of the window.



Menu	Submenu	Description
Monitoring	Sessions	Displays IPs and ports connected to the Data Server.
	Traffic Rate	Displays the Data Server network real time statistics in a table format
	History	Displays the Data Server network statistics accumulated yearly, monthly, weekly, and hourly in a graphic format
Statistics	Devices	Displays the network statistics of the Data Server for each device and for Tx and Rx.
	Protocols	Displays the network statistics of the Data Server for each protocol.
Serial State	-	Displays the current status of the serial line.
Services	-	Various functions of the Data Server are categorized into Security, Router, and Management, and the statuses of services are displayed in a table format.

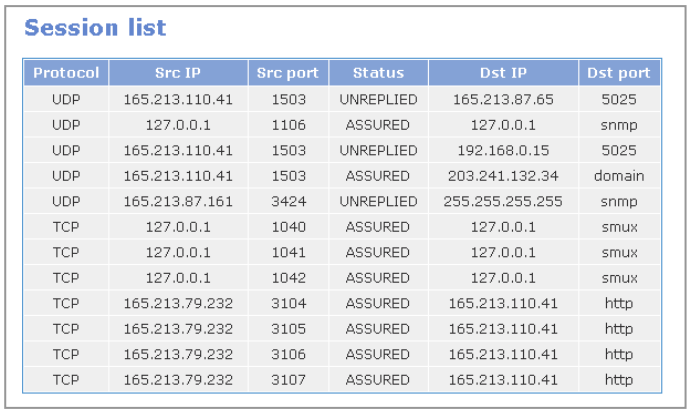
© SAMSUNG Telecommunications America, L.P.

Monitoring

The [Monitoring] menu displays the connection status of the Data Server, and the network statistics of the Data Server in real time or in values accumulated during a certain period.

Sessions

The [Sessions] menu displays information on IPs and ports connected to the Data Server.



Session list

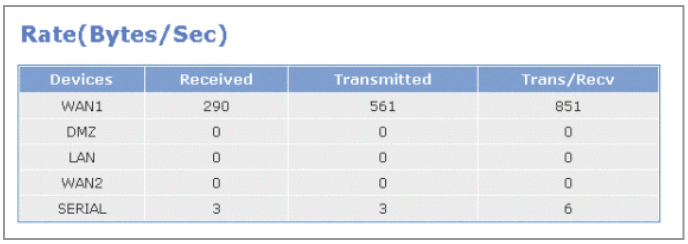
Protocol	Src IP	Src port	Status	Dst IP	Dst port
UDP	165.213.110.41	1503	UNREPLIED	165.213.87.65	5025
UDP	127.0.0.1	1106	ASSURED	127.0.0.1	snmp
UDP	165.213.110.41	1503	UNREPLIED	192.168.0.15	5025
UDP	165.213.110.41	1503	ASSURED	203.241.132.34	domain
UDP	165.213.87.161	3424	UNREPLIED	255.255.255.255	snmp
TCP	127.0.0.1	1040	ASSURED	127.0.0.1	smux
TCP	127.0.0.1	1041	ASSURED	127.0.0.1	smux
TCP	127.0.0.1	1042	ASSURED	127.0.0.1	smux
TCP	165.213.79.232	3104	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3105	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3106	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3107	ASSURED	165.213.110.41	http

Item	Description
Protocol	Type of protocol used for session connection(UDP, TCP)
Src IP	Source IP
Src Port	Source port
Status	- UNREPLIED: No response packets found on received packets that requires response - ASSURED: Response packet has occurred('UNREPLIED' changes to 'ASSURED')
Dst IP	Destination IP
Dst Port	Destination port

© SAMSUNG Telecommunications America, L.P.

Traffic Rate

Select [Monitoring] → [Traffic Rate] to display the network statistics of the Data Server in real time. Data is updated every 5 seconds.

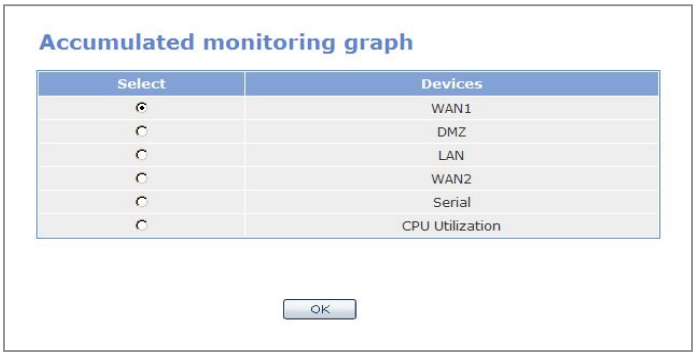


Rate(Bytes/Sec)

Devices	Received	Transmitted	Trans/Recv
WAN1	290	561	851
DMZ	0	0	0
LAN	0	0	0
WAN2	0	0	0
SERIAL	3	3	6

History

Select [Monitoring] → [History] to display the Data Server network statistics in values accumulated yearly, monthly, weekly, and hourly. The History is useful for analyzing the traffic patterns and trends on the network, and establishing the normal operating parameters.



Accumulated monitoring graph

Select	Devices
◉	WAN1
○	DMZ
○	LAN
○	WAN2
○	Serial
○	CPU Utilization

OK

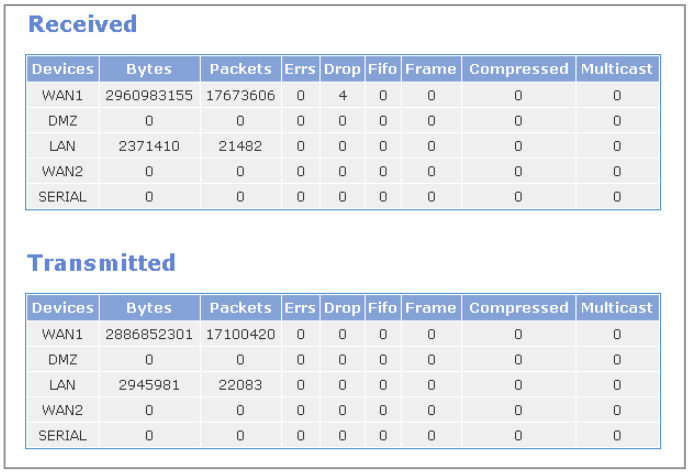
© SAMSUNG Telecommunications America, L.P.

Statistics

The [Statistics] menu displays the network statistics of the Data Server for each device and for each protocol.

Devices

Select [Statistics] → [Devices] to display traffic and error statistics showing bytes, packets, errors, drops, FIFO, Frame, Compressed, and multicast on the network. These statistics information is useful for detecting changes in traffic and error patterns of the network.



Received

Devices	Bytes	Packets	Errs	Drop	Fifo	Frame	Compressed	Multicast
WAN1	2960983155	17673606	0	4	0	0	0	0
DMZ	0	0	0	0	0	0	0	0
LAN	2371410	21482	0	0	0	0	0	0
WAN2	0	0	0	0	0	0	0	0
SERIAL	0	0	0	0	0	0	0	0

Transmitted

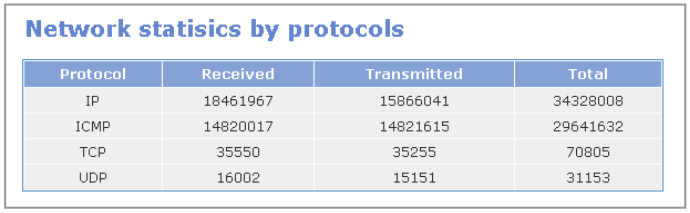
Devices	Bytes	Packets	Errs	Drop	Fifo	Frame	Compressed	Multicast
WAN1	2886852301	17100420	0	0	0	0	0	0
DMZ	0	0	0	0	0	0	0	0
LAN	2945981	22083	0	0	0	0	0	0
WAN2	0	0	0	0	0	0	0	0
SERIAL	0	0	0	0	0	0	0	0

Item	Description
Devices	Port type
Bytes	Total bytes received or transmitted
Packets	Total packets received or transmitted
Errs	Number of failed packets
Drop	Number of dropped packets
FIFO	FIFO queue is full (FIFO overrun)
Frame	Ethernet header type is invalid (Frame Alignment Error)
Compressed	Number of compressed packets
Multicast	Number of multicast packets

© SAMSUNG Telecommunications America, L.P.

Protocols

Select [Statistics] → [Protocols] to display the network statistics of the Data Server for the IP protocols, IP, ICMP, TCP, and UDP (Unit: Byte).

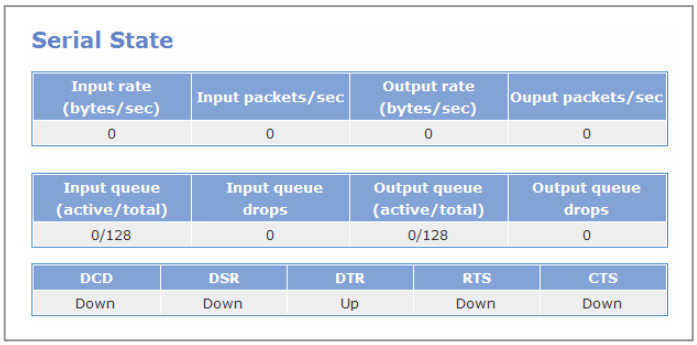


Network statisics by protocols

Protocol	Received	Transmitted	Total
IP	18461967	15866041	34328008
ICMP	14820017	14821615	29641632
TCP	35550	35255	70805
UDP	16002	15151	31153

Serial State

This function is used to display multiple data traffic and status of the serial line.



Serial State

Input rate (bytes/sec)	Input packets/sec	Output rate (bytes/sec)	Ouput packets/sec
0	0	0	0

Input queue (active/total)	Input queue drops	Output queue (active/total)	Output queue drops
0/128	0	0/128	0

DCD	DSR	DTR	RTS	CTS
Down	Down	Up	Down	Down

Item	Description
Input Rate	Indicates the input packet rate.
Input packets/sec	Indicates the number of input packets per second.
Output rate	Indicates the output packet rate.
Output packets/sec	Indicates the number of output packets per second.
Input queue	Indicates the number of packets waiting in the input queue / maximum size of the input queue.
Input queue drops	Indicates the number of packets dropped in the input queue or dropped in the serial network device
Output queue	Indicates the number of packets waiting in the output queue / maximum size of the output queue.
Output queue drops	Indicates the number of packets dropped in the output queue.
DCD	Data Carrier Detect. Indicates the detection results of carrier sent by DCE.
DSR	Data See Ready. Indicates the Tx/Rx setting status of DCE.
DTR	Data Terminal Ready. Indicates the Tx/Rx status of the DTE channel.

© SAMSUNG Telecommunications America, L.P.

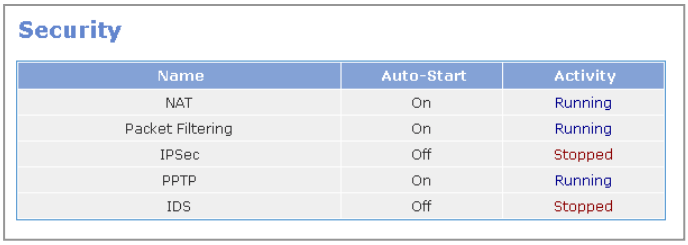
Item	Description
RTS	Request To Send. Indicates the status of the DTE Receive Mode.
CTS	Clear To Send. Indicates the status of Tx/Rx setting.

Services

The [Services] menu is used to display the statuses of security, router, and management services, provided by the Data Server.
If the 'Auto Start' item is checked 'On', the service will be started automatically when the system is rebooted. The 'Activity' item is set to 'Running' when the service is being provided, and is set to 'Stopped' when the service is not being provided.

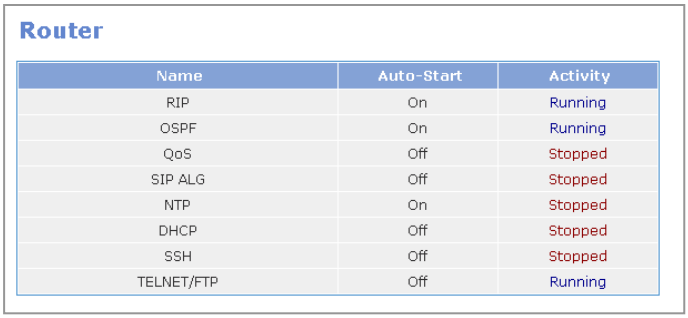
Security

This section displays the current status of security services: NAT, Packet Filtering, IPSec, PPTP, and IDS.



Router

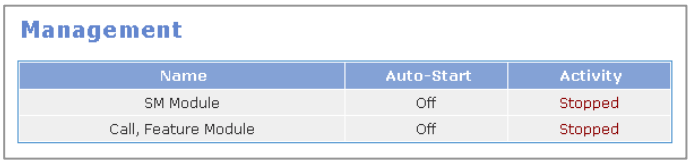
This section displays the current status of router services: RIP, OSPF, QoS, SIP ALG, NTP, DHCP, SSH, and TELNET/FTP.



© SAMSUNG Telecommunications America, L.P.

Management

This section displays the current status of management services: SM Module and Call, Feature Module.



VPN Menu

The VPN capability creates encrypted 'tunnels' through the Internet, allowing branch offices or remote users to securely connect into the network from off-site. VPN in OfficeServ 7200 Data Server supports both IPSec and PPTP solutions. The IPSec solution is supported for site-to-site (OS 7200 to OS 7200) connections and for individual remote access, allowing up to 100 secure tunnels. The PPTP solution is designed for remote client connection to OS 7200 only, a total of 25 PPTP connections are supported by OS 7200.

Please note that OS 7200 uses security processor (Hifn 7951) to implement the VPN functions such as tunneling through the data encryption, decryption, and authentication to enhance the system performance.

Select [VPN] to display the submenus of VPN on the upper left section of the window.

Menu	Submenu	Description
IPSec	Config	Sets IPSec.
	Management	Allows/Disallows execution of IPSec. Sets whether to execute IPSec when the system reboots.
	Certification	Creates and deletes the certification.
	Status	Checks if IPSec tunnel is properly connected.
PPTP	Config	Sets PPTP.
	Management	Allows/Disallows execution of PPTP. Sets whether to execute PPTP when the system reboots.

Setting VPN Client in Windows XP/2000

OfficeServ 7200 Data Server supports Microsoft Windows PPTP and IPSec VPN clients. Please refer to 'APPENDIX A' for detailed information on configuring MS Windows IPSec VPN client.

IPSec

IPSec (IP Security) is the Internet standard protocol for tunneling, encryption, and authentication.

IP Security Protocol (IPSec) provides security services in the IP layer through implementing Internet Key Exchange (IKE). IKE is an automatic keying mechanism, requiring two phases in establishment of a VPN tunnel. Phase one establishes the Internet Security Association Key Management Protocol (ISAKMP) tunnel that manages Phase two IPSec data tunnel. OfficeServ 7200 IPSec supports the following parameters:

- Encryption cipher: DES or 3DES
- Modes: Main
- Keys: Pre-shared or Certificates
- Hash algorithm: MD5 or SHA1
- Transforms: Automatic Header (AH) or Encapsulation Security Payload (ESP)
- Diffie-Hellman Group: Group 2
- Perfect Forward Security (PFS): On or Off

OfficeServ 7200 supports the following three authentication methods:

- RSA key – for OS 7200 to OS 7200 connections only. A RSA key is literally a long string of alphanumeric characters, which is the encoding of a public key. OS 7200 can create new RSA key by selecting Create New Host Key under IPSec Management menu.
- Pre-shared key – pre-shared key is simply non-encrypted passphrases stored in plain-text. This is used to set up the connection with easy authentication.
- X.509 certificate – the X.509 certificate has the same encryption scheme as RSA keys with certificates. The certificate contains useful auxiliary information and it allows a trust-inheritance scheme.

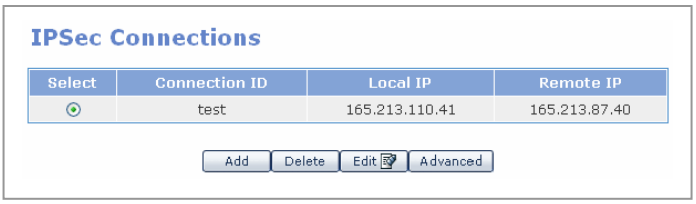
OfficeServ 7200 supports Gateway to Gateway and Client to Gateway tunnels, allowing up to a total of 100 tunnels. In the case of Gateway to Gateway tunnel configuration, in order to establish a secure communication over the Internet with the remote site, both local gateway and remote gateway should have the matching VPN parameters. The local VPN parameters on one end must match the remote VPN parameters on the other end, and vice versa.

IPSec Tunnel Mode

OfficeServ 7200 Data Server supports the IPSec tunnel mode only, it does not support the Transport mode. If the WAN interface is used for serial, IPSec is not supported. Since the serial line is used as leased line, you need not use IPSec for security.

Config

Users are allowed to add, delete, and search an IPSec tunnel on the [IPSec] → [Config] menu, and to set detailed items.

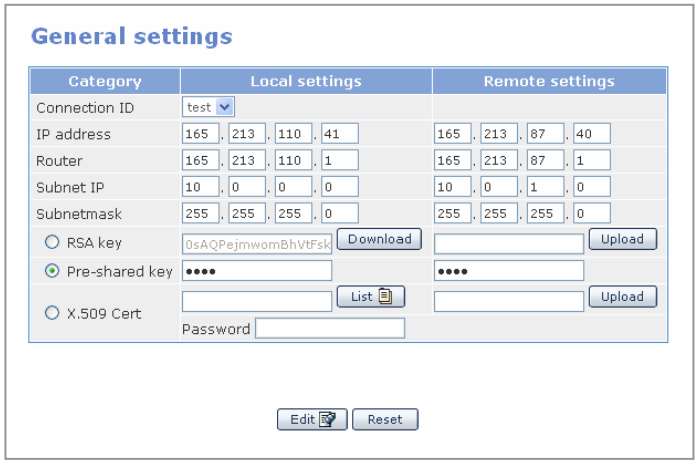


The menu buttons are defined as shown below:

Button	Description
Add	Creates IPSec tunnel
Delete	Deletes IPSec tunnel
Edit	Modifies IPSec tunnel data
Advanced	Sets detailed items of IPSec tunnel

Add

Click the [Add] button from the <IPSec Connections> window to display the window below: Enter each item value and click the [Add] button to add an IPSec tunnel.



Category	Description
Connection ID	ID composed of certain letters(Required)
IP Address	External IP address(Required)
Router	Router IP address
Subnet IP	Internal IP address
Subnetmask	Internal subnetmask

Category	Description
RSA Key/ Pre-shared Key /X.509 Cert	Selects host authentication method - RSA Key: Public key is RSA key of Local settings. Click the [Download] button to store RSA key to your PC, and send it to other PC through a path. After RSA key of Remote settings receives file in the target PC through a path, click the [Upload] button to enter a key value. - Pre-shared Key: Authentication method entering password. - X.509 Cert : Authenticate using your own certification and the CA certification. In the Local settings side, enter the file name of your own certification directly, or click the [List] button and select from the current authentication list.(If you select the Certification, the Advanced Left ID is automatically entered). In the Remote settings side, click the [Upload] button to upload the CA Certification of the other party. You can check the host certification registered in Local and integrity.

If the ‘Router’ item value is not entered, the ‘IP address’ item of the Local settings and Remote settings will be used as the ‘Router’ item.

If the ‘Subnet IP’ item value and the ‘Subnetmask’ item value are not entered in the Remote settings, the security tunnel between local subnet and remote host will be added. Then, remote IPSec client can operate as a part of local subnet.

Setting Router Value

If the IP address(in other words, the result of netmasking the IP Address)of ‘Local settings’ is the same as the ‘IP Address’ of ‘Remote settings’, enter the ‘IP Address’ of ‘Remote settings’ in the ‘Router’ of ‘Local settings’, and enter the ‘IP Address’ of ‘Local settings’ in the ‘IP Address’ of ‘Remote settings’.

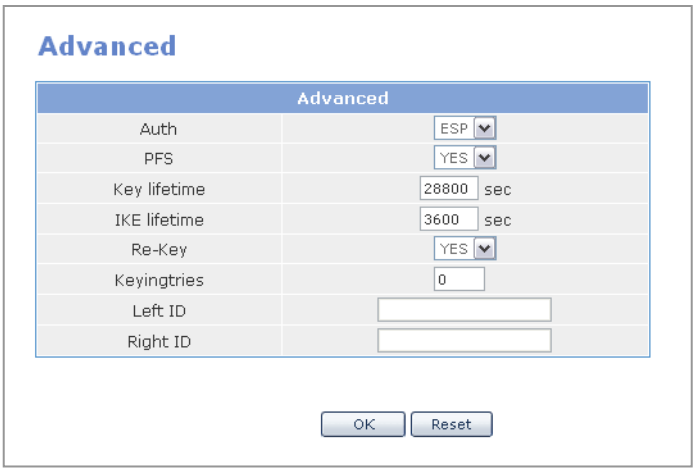
Setting Connection ID

Connection ID should be English alphabets or the combination of English alphabets and numbers, and the first letter should start with English alphabet.(ID should not be configured using numbers only.)

Advanced

Click the [Advanced] button from the <IPSec Connections> window to display the window below: Detailed items of IPSec can be set.

The 'Advanced' menu is set only if the authentication is performed using X.509 Cert.



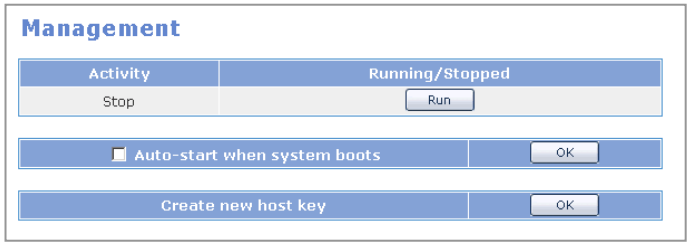
Item	Description
Auth	Select packet authentication protocol. - Authentication Header (AH): Allows data sender authentication. - Encapsulating Security Payload (ESP): Allows sender authentication and data encryption.
PFS	Perfect Forward Secrecy; select whether to use the security for session key delivery -YES, by default it is set to 'yes'. - NO. Set to NO if the system is connected to a third party client software that does not support PFS.
Key lifetime	Cycle of newly added key used in packet encryption through repeated IKE 2 level.
IKE lifetime	IKE duration time If duration time passes, host authentication (IKE 1 level) is performed again.
Re-Key	Set whether to add a new key(whether to add a new key and negotiate again in the IKE 2 level).
Keyingtries	Retry count of key exchange when encryption key exchange fails in the IKE 2 level.
Left ID	Set ID if ID as well as IP address is required. Typically, IP address is used for authenticating other host in the IKE 1 level.
Right ID	Set ID if ID as well as IP address is required. Typically, IP address is used for authenticating other host in the IKE 1 level.

© SAMSUNG Telecommunications America, L.P.

You may change the values of PFS or Key lifetime for compatibility with other systems. If 'Left ID' and 'Right ID' are not set, the IP address replaces the value.
In X.509, enter the subject of a certification in 'Left ID' and 'Right ID' of 'advanced'.

Management

The user allows/disallows executing IPSec services on the [IPSec] → [Management] menu. Check the 'Auto-start when system boots' item, and click the [OK] button to execute the IPSec services automatically while the system reboots.

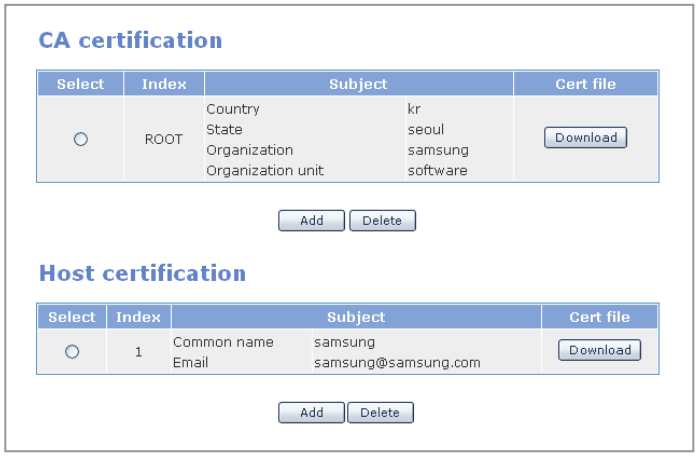


Click the [OK] button of the 'Create new host key' item to add a new RSA (public key password method) key. Use this menu to add a new RSA key if the host authentication method of RSA key used.

© SAMSUNG Telecommunications America, L.P.

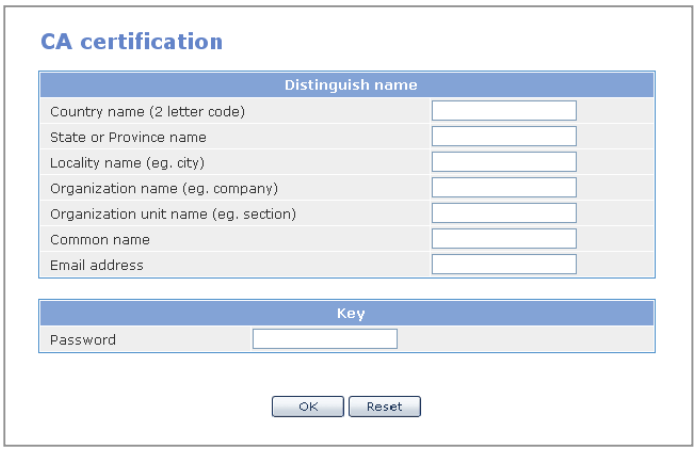
Certification

This function is used to issue/delete/download the CA certification and host certification, and to view a list of current certification.

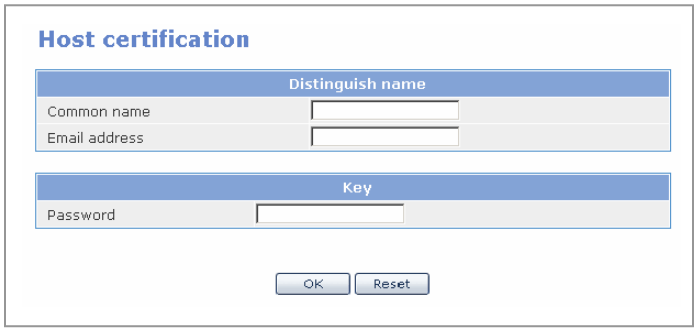


The table below explains the menu buttons:

Item	Description
(CA) Add	Creates the CA certification
(CA) Delete	Deletes the CA certification
(Host) Add	Creates the host certification
(Host) Delete	Deletes the host certification



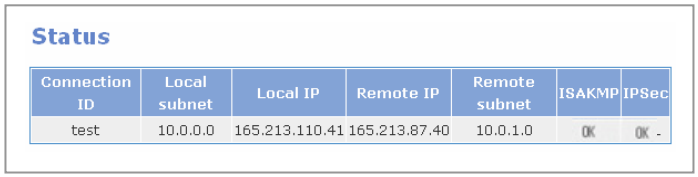
Item	Description
Country name	Country name(2 characters ex. kr, cn)
State or Province name	State or province name
Locality name	Locality name
Organization name	Company name
Organization unit name	Organization(department) name
Common name	User Name
Email address	email address
Password	Certification password



Item	Description
Common name	User Name
Email address	email address
Password	Certification password

Status

Users are allowed to check if the target IPSec tunnel is connected properly on the [IPSec] → [Status] menu.

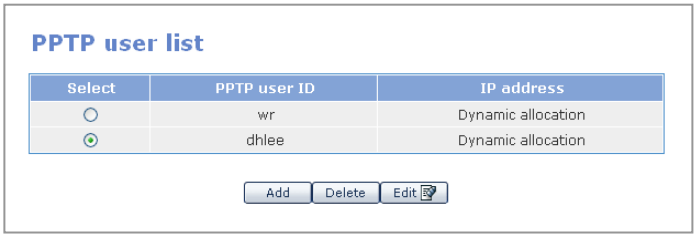


PPTP

Point to Point Tunneling Protocol, PPTP, is a proposed standard sponsored by Microsoft as an extension of the Internet's Point-to-Point Protocol. Any user of a PC with Windows 98 or above is able to use an Internet service provider to connect securely to OfficeServ 7200 data network. Since PPTP setting is convenient compared with IPSec and the client S/W is provided by Windows OS, the user can use VPN functions easily. OS 7200 supports a total of 25 PPTP connections.

Config

Users are allowed to add, edit, delete, and search VPN tunnel data on the [PPTP] → [Config] menu, and to set detailed items.



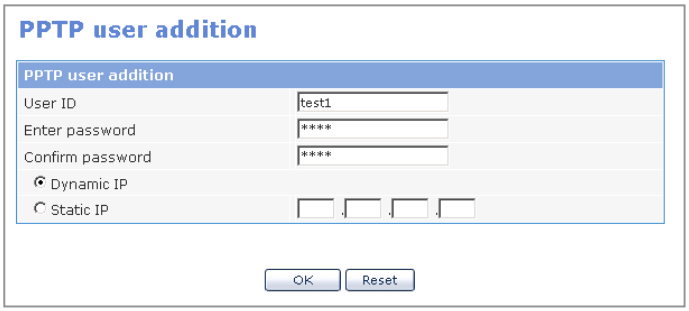
The menu buttons are defined as shown below:

Button	Description
Add	Create PPTP users
Delete	Delete PPTP users
Edit	Modify PPTP user data

© SAMSUNG Telecommunications America, L.P.

Add

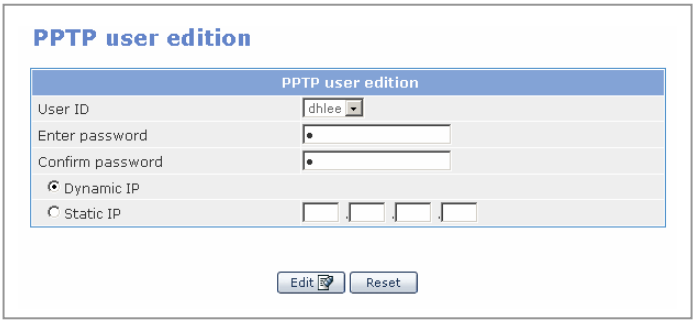
Click the [Add] button from the <PPTP user list> window. Enter each item value and click the [OK] button to add a PPTP user. IP assignment to remote client could use either dynamic IP or static IP.



Item	Description
User ID	ID composed of certain letters
Password	Shared password
Dynamic IP	Enter dynamic IP to remote client
Static IP	Enter static IP to remote client(Enter IP address)

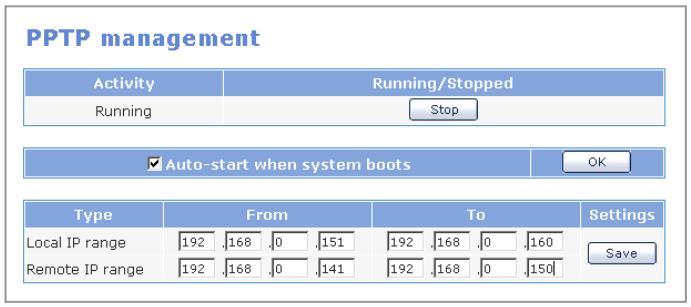
Edit

Click the [Edit] button from the <PPTP user list> window. Then, the window below appears. Enter each item value and click the [OK] button to edit VPN tunnel data.



Management

The user allows/dis-allows executing PPTP services on the [PPTP] → [Management] menu. Check the 'Auto-start when system boots' item and click the [OK] button to execute the PPTP services automatically while the system reboots.



Users are allowed to set the IP range of the remote client that uses dynamic IP in the 'Local IP range' item, and set the IP range of PPP daemon responsible for remote client in the 'Remote IP range' item.

CAUTION

Setting IP Range

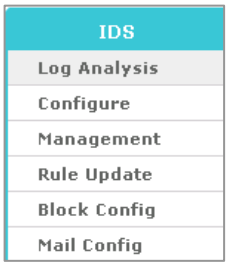
The number of IPs for the 'Local IP range' and that for the 'Remote IP range' should be identical. For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

© SAMSUNG Telecommunications America, L.P.

IDS Menu

OfficeServ 7200 Intrusion Detection System is based on the open source, network intrusion detection software Snort. IDS service is capable of performing real-time traffic analysis and packet logging on IP networks. It provides defense by analyzing network traffic, blocking, or alerting when suspicious activity is detected. IDS rules can be downloaded and updated from the Snort website .IDS service can be activated on all WAN interfaces. In order to start the IDS service, Packet Filtering under the [Firewall/Network] must be activated first.

Select [IDS] to display the submenus of IDS on the upper left section of the window.

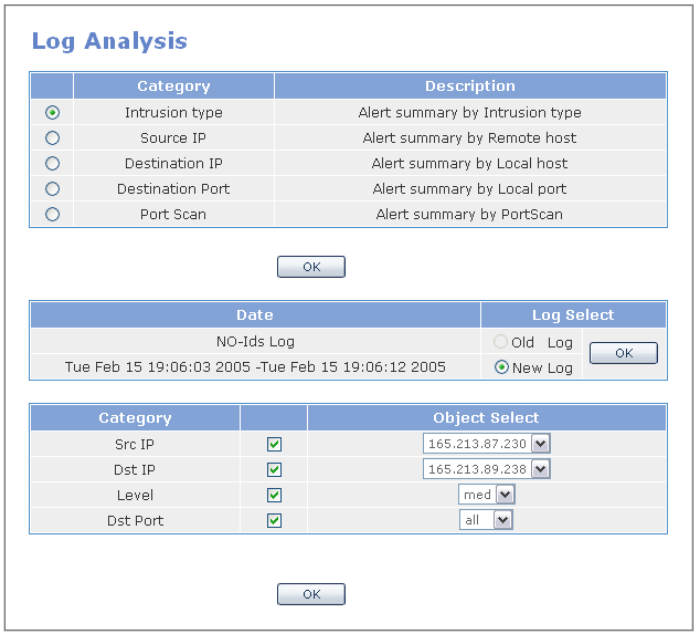


Menu	Description
Log Analysis	Analyzes logs detected by IDS rule.
Configure	Sets whether to apply Config file and Rule file before executing IDS.
Management	Allows/Disallows IDS implementation. Set IDS to be executed when the system reboots.
Rule Update	Updates new rules downloaded from the Web.
Block Config	Sets Source IP detected by IDS to be blocked by a firewall.
Mail Config	Sets to send IDS message when IDS detects.

© SAMSUNG Telecommunications America, L.P.

Log Analysis

Analyze the logs detected by Intrusion Detection System (IDS) rule on the [Log Analysis] menu. Select the target Category to be analyzed, and click the [OK] button to display the corresponding log analysis for the category.



Category	Item	Description
Category	Intrusion type	Analyzes logs detected for IDS rule types.
	Source IP	Analyzes logs for Source IP detected by IDS.
	Destination IP	Analyzes logs, detected by IDS, of the OfficeServ 7200 external IP(WAN1, WAN2, SERIAL).
	Destination Port	Analyzes logs when the destination IP of a log detected by IDS is the port of an external IP(WAN1, WAN2, SERIAL).
	Port Scan	Analyzes the logs if the logs detected by IDS have port scan type.
Date	-	Time to record a log.
Log Select	Old Log	Analyzes old logs.
	New Log	Analyzes the IDS log based on the latest log.

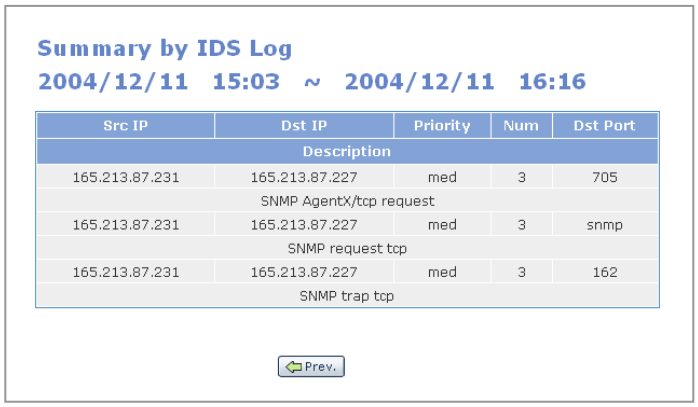
© SAMSUNG Telecommunications America, L.P.

Select ‘Old Log’ and click [OK] to analyze old logs. Then, data on the old logs will be displayed in ‘Object Select’.

Select ‘New Log’ and click [OK] to analyze the latest logs. Then, data on the latest logs will be displayed in ‘Object Select’.

The default is ‘New Log’. If an IDS log does not exist, the ‘NO-Ids Log’ message will be displayed.

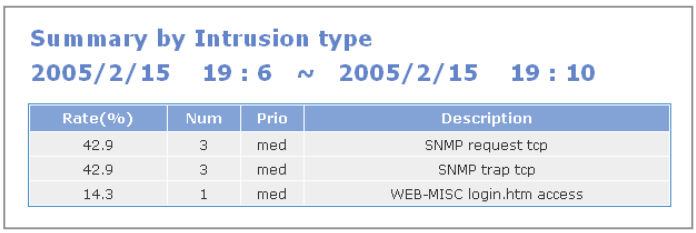
Select ‘Old Log’ or ‘New Log’ from the <Log Analysis> window and then, select an option from ‘Object Select’. Then, click [OK] to analyze the log and display the results. The window below shows the results of analyzing the log for Src IP (165.213.87.231).



Item	Description
Src IP	Displays the source IP of the detected log, which is the attacker IP address.
Dst IP	Displays the destination IP of the detected log, which is the attacked IP address.
Priority	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Num	Displays the count of attacks whose types are displayed in ‘Description’.
Dst Port	Displays the destination IP.
Description	Displays attack types.

Intrusion type

Check 'Intrusion type' from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.



Summary by Intrusion type

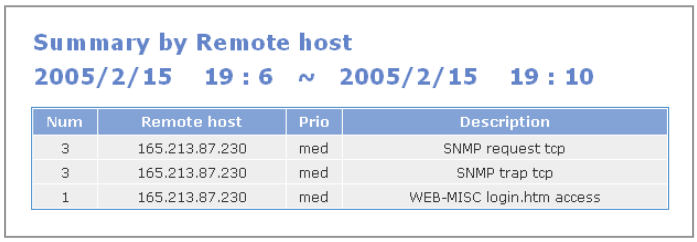
2005/2/15 19 : 6 ~ 2005/2/15 19 : 10

Rate(%)	Num	Prio	Description
42.9	3	med	SNMP request tcp
42.9	3	med	SNMP trap tcp
14.3	1	med	WEB-MISC login.htm access

Item	Description
Rate(%)	Monitors logs detected by IDS according to type and displays logs as rate(%).
Num	Number of logs detected by IDS according to type
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

Source IP

Check 'Source IP' from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.



Summary by Remote host

2005/2/15 19 : 6 ~ 2005/2/15 19 : 10

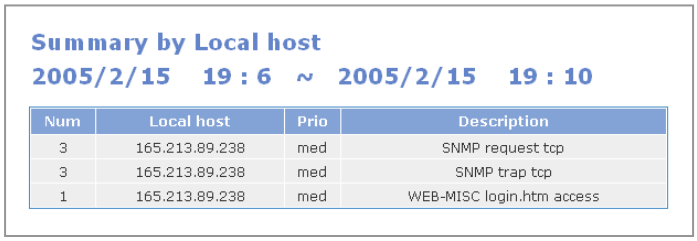
Num	Remote host	Prio	Description
3	165.213.87.230	med	SNMP request tcp
3	165.213.87.230	med	SNMP trap tcp
1	165.213.87.230	med	WEB-MISC login.htm access

© SAMSUNG Telecommunications America, L.P.

Item	Description
Num	Number of logs detected by IDS for Source IP attacking the logs
Remote host	Host IP attacking logs detected by IDS
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

Destination IP

Check 'Destination IP' from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.

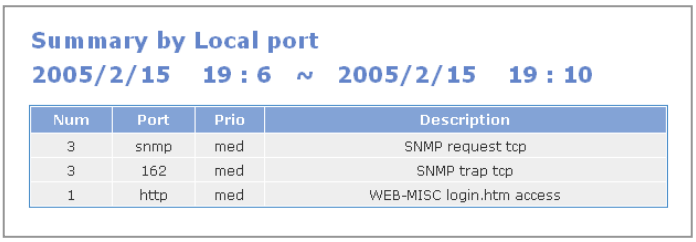


Item	Description
Num	Number of logs detected by IDS according to attacked Destination IP
Local host	Attacked host IP of logs detected by IDS
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

© SAMSUNG Telecommunications America, L.P.

Destination Port

Check ‘Destination Port’ from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.


Summary by Local port
2005/2/15 19 : 6 ~ 2005/2/15 19 : 10
Num Port Prio Description
3 snmp med SNMP request tcp
3 162 med SNMP trap tcp
1 http med WEB-MISC login.htm access

Item	Description
Num	Numbers of detected by IDS according to port when attacked Destination IP is a network(e.g., LAN or DMZ)
Port	Attacked host IP of logs detected by IDS
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

Port Scan

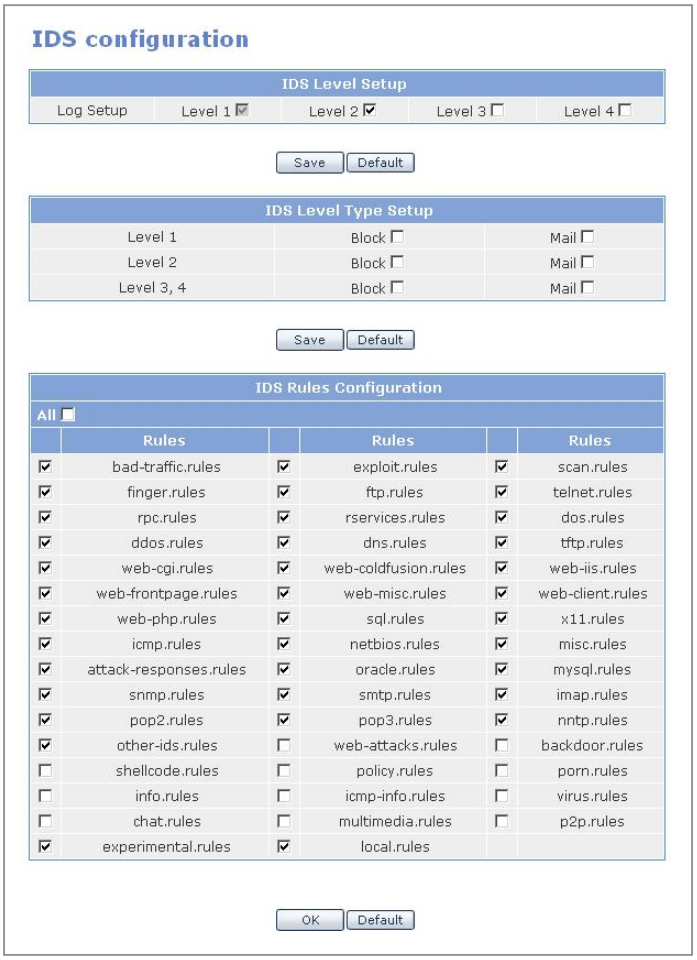
Check ‘Port Scan’ from the Category item of the <Log Analysis> window and click the [OK] button to display the Log Analysis window below: Date indicates the time from the first detection to the last detection.

Item	Description
ports	Number of TCP and UDP ports, which scanned ports in logs detected by IDS.
Hosts	Number of host scanned a port in logs detected by IDS.
Remote host	IP tried port scan.

© SAMSUNG Telecommunications America, L.P.

Configuration

Set whether to apply Config file and Rule file before IDS implementation on the [Configuration] menu. After checking the risk level on the IDS Level Setup, click the [Save] button and go to IDS Rules Configuration to select rules. Last click the [OK] button to apply the rules to IDS Configuration file and to start IDS daemon.



- IDS Level Setup: Categorized into the following four levels depending on risk level:

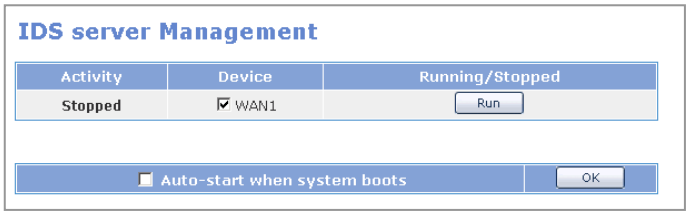
Level setup	Risk	Description
Priority 1	The highest risk(high)	Only Priority 1 is detected by IDS Rules.
Priority 2	Mid risk(med)	Priority 1 and 2 are detected by IDS Rules.
Priority 3	Mid risk(med)	Priority 1, 2 and 3 are detected by IDS Rules.
Priority 4	Low risk(low)	Priority 1, 2, 3 and 4 are detected by IDS Rules.

- IDS Level Type Setup: Select a function in each level and click [OK].
- Level 1: By default, performs the log and alarm functions. Selects whether to disconnect the detected source IP and/or to send a mail to the manager.
- Level 2: By default, performs the log function. Selects whether to disconnect the detected source IP and/or to send a mail to the manager.
- Level 3, 4: By default, performs only the log function. Selects whether to block the access to the detected source IP and/or to send a mail to the administrator.
- IDS Rules Configuration: Sets rules that will be detected in IDS. Select the check box of the corresponding rule, and click the [Save] button to set the target site or rule to be detected. If the ‘All’ item is checked, all rules will be selected.

© SAMSUNG Telecommunications America, L.P.

Management

The user allows/disallows executing IDS on the [Management] menu. Check the 'Auto-start when system boots' item and click the [OK] button. Then the IDS service automatically executed when the system reboots.



Item	Description
Activity	- Running: IDS is operating. - Stopped: IDS is not operating.
Device	Select equipment for applying IDS. Equipment is limited to WAN used for setting firewall, and number of equipment is displayed as much as that of external network, which is set when a firewall is installed.
Running/Stopped	Click the [Run] button. Then, IDS is executed. Click the [Stop] button. Then, IDS is not executed.
Auto-start when system boots	If this item is checked and the [OK] button is clicked, IDS is executed automatically while the system reboots. However, firewall is not executed while the system reboots, the IDS does not operated.

© SAMSUNG Telecommunications America, L.P.

Rule Update

Users are allowed to update new IDS rules on the [Rule Update] menu. Enter the target address in the 'Path' item, and click the [OK] button to download new rules.

- Current rule information: Displays the version of a rule and the time distributed.
- Rule update path: Enter the target address to download new IDS rules. When entering the target URL address, omit 'http://' as shown above.
- Default address is set to 'www.snort.org/pub-bin/oinkmaster.org (IDS <snort> official website)'.
- Updating a version is executed when the update is required after the current version is compared with the version to be updated.

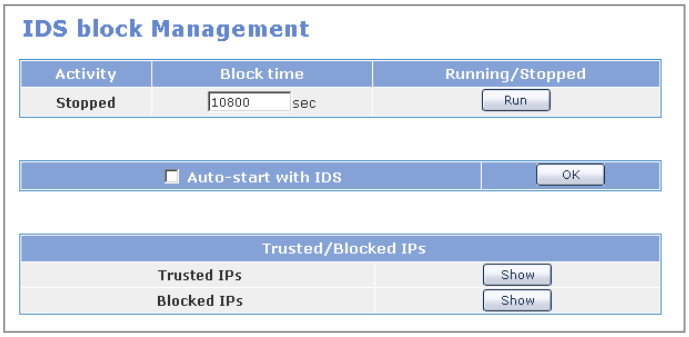
CHECK

When Rules are not Updated

If Domain Name Server(DNS) address is not entered when a firewall is installed, update is not executed. Thus, check if the DNS address is entered when the rule is not updated.

Block Config

Set to block the source IP which is detected by IDS on the [Block Config] menu, using system firewall. This function can be performed when the IDS are operating.



Item	Description
Activity	- Running: IDS Block server is operating. - Stopped: IDS Block server is not operating.
Block time(sec)	Set the time to block source IP detected by IDS. After this item is set and DS Block server is executed, source IP is blocked for a certain period of time set in this item, and deleted from Blocked IP List after timeout. Defaults value of block time is '10800'.
Running/ Stopped	Click the [Run] button. Then, IDS Block server operates. Click the [Stop] button. Then, IDS Block server does not operate.
Auto-start when system boots	If this item is checked and the [OK] button is clicked, IDS is executed automatically while the system reboots. However, firewall is not executed while the system reboots, the IDS is not executed.

© SAMSUNG Telecommunications America, L.P.

Trusted IPs

Click the [Show] button from the 'Trusted IPs' item of the <IDS block Management> window to display the window below: If the source IP detected by IDS is trusted, enter the target IP(or Network) and click the [Add] button to register the IP(or Network).

Since internal network is registered with Trusted IPs, the internal network or WAN IP does not need to be registered. However, trusted IP(or Network) from external IPs should be registered. If IDS detected improper usage and block the external user from accessing the network, the corresponding IP(or Network) of the external user should be registered.

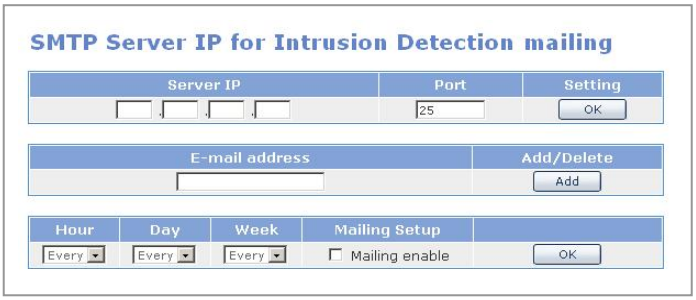
Blocked IPs

Select 'Blocked IPs' of the <IDS block Management> window to display the window below: The IP blocked by the IDS block server or detected by IDS is displayed.

© SAMSUNG Telecommunications America, L.P.

Mail Config

Set to send alarm messages (IDS logs) to the administrator when IDS is detected on the [Mail Config] menu.



Item	Description
Server IP	IP address of mail server Install mail server into internal network (e.g., LAN or DMZ) and enter internal IP.
Port	Simple Mail Transfer Protocol(SMTP) service port of mail server Typically port 25 is used.
E-mail address	Administrator's email address, which will be received alarm messages(e.g., aaa@samsung.com) Click the [Add] button to register the email address. Click the [Delete] button to delete the registered email address.
Mailing enable/disable	Check this item and click the [OK] button to send alarm messages(IDS log) to the target registered email address. Set the time period on an hourly, daily, or weekly basis. Then, according to the setting period, an alarm message(IDS log) can be sent periodically.

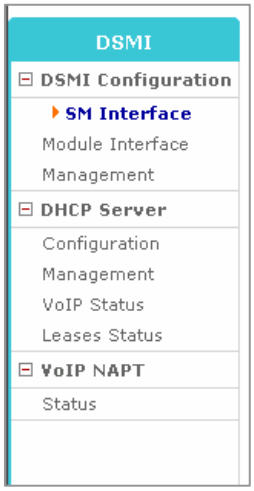
© SAMSUNG Telecommunications America, L.P.

DSMI Menu

DSMI menu provides the following services:

- Configuring Data Server Manager Interface (DSMI) communicating with the VoIP services provided by OfficeServ 7200. In OS 7200, MCP processes VoIP signaling and MGI processes the VoIP media. If MCP and MGI are configured with private IP addresses, and they are installed behind the WIM NAT router with fixed public IP address for the WAN interface, DSMI could be activated to perform NAPT for signaling and media data packets for VoIP service.
- Displaying the VoIP status
- Displaying VoIP NAPT setting
- Configuring DHCP for PCs and IP Telephones operating in DHCP Client mode.

Select [DSMI] to display the submenus of DSMI on the upper left section of the window.



Menu	Submenu	Description
DSMI Configuration	SM Interface	Sets the item related with message data transmission to communicate with System Manager(SM).
	Module Interface	Sets the environment for the communication between the Call Server and the Feature Server.
	Management	Sets to execute the program to communicate among SM Interface, Call Server, and Feature Server, to stop the program, or to execute the program when the system restarts.

© SAMSUNG Telecommunications America, L.P.

(Continued)

Menu	Submenu	Description
DHCP Server	Configuration	Sets the internal network to operate the DHCP Server, and IP pool for a DHCP terminal. IP pool can be set for the Call Server, Feature Server, MGI, IP Phone, SIP Phone, and normal data terminal.
	Management	Allows/Disallows executing DHCP Server. Set DHCP Server to be executed when the system reboots.
	VoIP Status	When a program is executed for the communication with the Call Server or Feature Server, this indicates the IP terminal information of the OfficeServ 7200 system received from the Call Server or Feature Server.
	Leases Status	Displays a list of the IPs leased by the DHCP Server to each client.
VoIP NAPT	Status	Displays the static NAPT information for the OfficeServ 7200 VoIP service. When a program is executed for the communication with the Call Server and with Feature Server, this information is automatically set. After the setting is completed, the information is displayed.

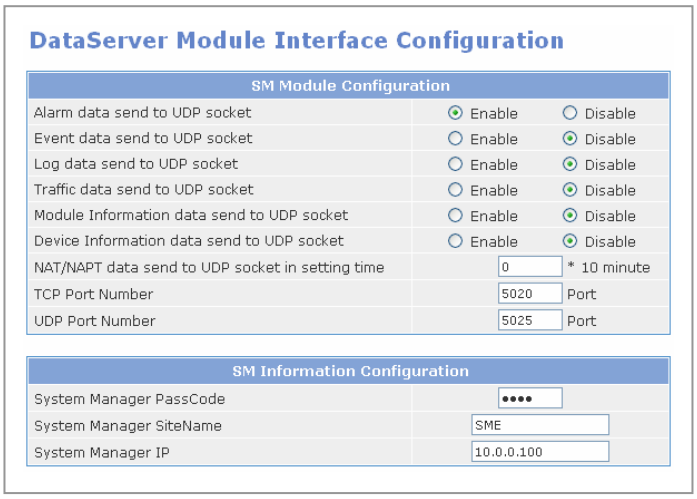
© SAMSUNG Telecommunications America, L.P.

DSMI Configuration

Set Data Server Module Interface (DSMI) environment on the [DSMI Configuration] menu.

SM Interface

System Manager is a network management tool which will be available in the future release. This menu is reserved for the future usage once the System Manager application is available. The item related with message data transmission for the communication with System Manager(SM) can be set in the [SM Interface] menu. Since the network traffic and system are overloads when much message data is transferred, the user should control whether to transfer message data and transmission interval.



If message data is sent based on UDP, select whether to send the data as shown above. If message data is sent based on TCP, the user is not required to select whether to send the data because messages data is sent when the system manager requires.

Since the TCP port is set to ‘5020’ and the UDP port is set to ‘5025’, the value should not be changed.

Information on the SM Manager can be entered. This window displays the information received from the Call Server.

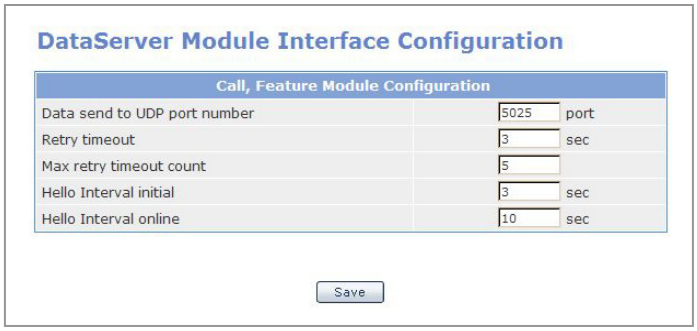
© SAMSUNG Telecommunications America, L.P.

Category	Item	Description
SM Module	Alarm data	When 'Enable' is set, alarm message, which occurs when the system is abnormal or a hacker attacked the system, is sent to the system manager through UDP port immediately.
	Event data	When 'Enable' is set, system event message being generated is sent to the system manager through UDP port immediately.
	Log data	When 'Enable' is set, message data is sent to the system manager through UDP port immediately when the user access the system through system connection path.
	Traffic data	When 'Enable' is set, network traffic data generated from system network equipment is sent to the system manager through UDP port on a regular basis (30 minutes).
	Module Information data	When 'Enable' is set, system module data is sent to the system manager through UDP port.
	Device Information data	When 'Enable' is set, system network equipment data is sent to the system manager through UDP port.
	NAT/NAPT data	Sets the time interval for sending IP data and connection data, which use NAT/NAPT from clients being connected to the system manager. For example, '5' is entered, the data is sent every 50 minutes.
	TCP Port Number	Sets the TCP connection port with the system manager. The default is 5020.
	UDP Port Number	Sets the UCP connection port with the system manager. The default is 5025.
SM Information	System Manager Passcode	Displays the passcode of the system manager received from the Call Server. The passcode may be forced to be set.
	System Manager Sitename	Displays the site name of the system manager received from the Call Server. The name may be forced to be set.
	System Manager IP	Displays the IP of the system manager received from the Call Server. The IP may be forced to be set.

© SAMSUNG Telecommunications America, L.P.

Module Interface

The program environment for the communication with the Call Server or with Feature Server can be set in the [Module Interface]. When the system reboots, default value is set as shown below:

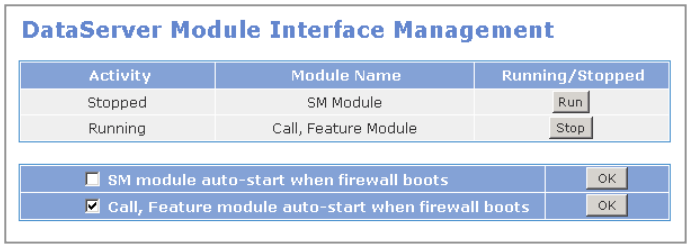


Item	Description
Data send to UDP port number	UDP port information for the communication with the Call Server or Feature Server. Default is '5025'.
Retry timeout (Sec)	DSMI_CF, Call Server, Feature Server, and Data Server communicate based on UDP. Since UDP may lose packet, it requests retry when it does not receive the requested data. Set time interval for retry. For example, the item is set to '3'. After a packet is lost, retry is requested, but the requested data is not received. Then, UDP requests retry 3 seconds later. If the requested packet is not received for 3 seconds, timeout occurs.
Max retry timeout count	Sets retry count when packet is lost continuously while DSMI_CF exchanges data with Call Server and Feature Server. For example, Retry timeout is set to '3' and '5', retry is requested five times for three seconds. If requested packet is not received, stop retry request.
Hello Interval initial	Hello massage is the message that DSMI_CF, Call Server and Feature Server exchanges periodically. Set time interval for sending Hello message.
Hello Interval online	The programs for the Call Server and Feature Server send the Hello message at intervals of the setting value set in the 'Hello Interval initial' item to check the link information of the other party and to notify the status of the program during restart. When Hello message is received from Call Server and Feature Server while Hello message is sent, Hello message should be sent every certain time period set in this item. This value should be set to be more than the value of 'Hello Interval initial' item.

© SAMSUNG Telecommunications America, L.P.

Management

Program for the communication with SM or the communication with the Call Server or Feature Server can be executed or be stopped through the [Management] menu. Check the 'Auto Start' item. Then, the corresponding program starts automatically when the system reboots.



Check the 'SM module auto-start when firewall system boots' or 'Call, Feature module auto-start when firewall system boots' item and click the [OK] button. Then, the SM interface program or the Call, Feature interface program is automatically executed.

DHCP Server

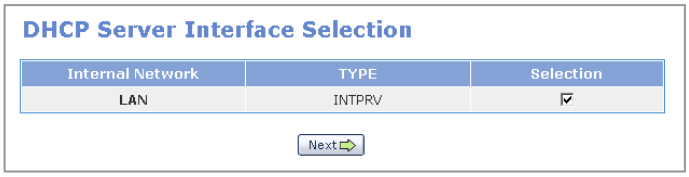
OfficeServ 7200 provides DHCP service to network clients. This service dynamically assigns IP addresses to network data terminals or Samsung IP telephones, so you do not need to manually assign an IP address to each one.

Set equipment to operate the DHCP Server on the [DHCP Server] menu and allow or disallow the DHCP Server operation.

Configuration

Select equipment for operating DHCP Server from internal network equipment set on the [Firewall/Network] menu on the [Configuration] menu.

Select the [DHCP Server] → [Configuration] menu to display the internal network set to 'Internal Private Network' or 'Internal Public Network' on the [Firewall/Network] → [Management] → [Configuration] menu.



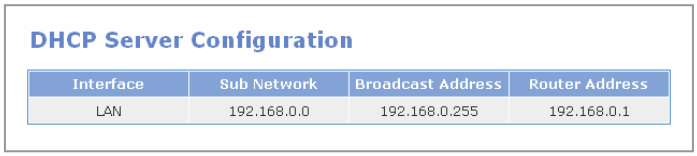
Check the check box to be set and click the [Next] button to display the <DHCP Server Configuration> window to set the environment.

The <DHCP Server Configuration> window displays default value of the equipment selected from the <DHCP Server Interface Selection> window. Allocate the OfficeServ 7200 system IP such as Call Server whose subnet is the same level with that of the selected equipment, Feature Server, IP phone, SIP phone, and data terminal to DHCP.

Set the following items and click the [Save] button.

DHCP Server

Displays normal data to be allocated to DHCP client.

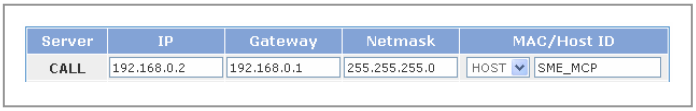


© SAMSUNG Telecommunications America, L.P.

Item	Description
Sub Network	Sub network data Value set on the [Firewall/Network] → [Management] → [Config] menu. This value can be changed on the menu.
Broadcast Address	Broadcast address Value set on the [Firewall/Network] → [Management] → [Config] menu. This value can be changed on the menu.
Router Address	Router address Value set on the [Firewall/Network] → [Management] → [Config] menu. This value can be changed on the menu.
Default Lease Time(sec)	If DHCP client does not request expiration time, the value will be allocated to this item.
MAX Lease Time(sec)	If DHCP client requests expiration time, the value is the maximum time to be allocated.

CALL Server

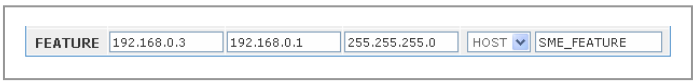
Sets the Call Server MCP IP setting, which should be identical to MMC 830 MCP Ethernet Parameter. If the Call Server operates in DHCP mode, select the 'Host' option (which will be automatically set to 'SME_MCP') to allocate an IP address to the Call Server.



Item	Description
IP	Call Server IP address
Gateway	Gateway data
Netmask	Netmask data
MAC/Host ID	Client authentication type - NONE: Executes DHCP IP request without authentication. - MAC: Authentication as MAC - HOST: Authentication as HOST ID (Default value: SME_MCP)

Feature Server

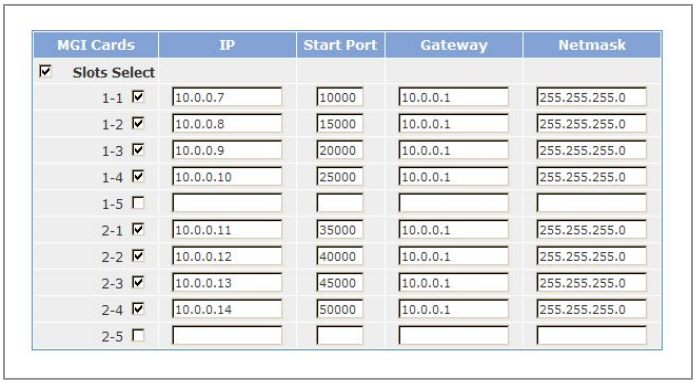
Feature Server is reserved for the future IP UMS application release. Set the IP of the Feature Server. When the Feature Server operates in DHCP mode, select the 'Host' option (which will be automatically set to 'SME_FEATURE') to allocate an IP address to the Feature Server.



MGI Cards

Set the location and IP address of the MGI card mounted on the system.

- MGI Cards Slots Select: check the cabinet-slot location of MGI card installed on the system. OfficeServ 7200 can support up to 10 MGI cards.
- IP/Gateway/Netmask: Set the IP address of the MGI card. The IP setting should be identical to MMC 831 - MGI Parameter.
- Start Port: Start Port is used by each MGI when the card is configured as private with public IP of the WAN. Each MGI must have different start ports. If these values are not manually configured, system will automatically set the default values starting from 10000 and increase by 5000 according to the cabinet or slot order. Once DSMI is activated, network address port translation will automatically forward the MGI's default 32 public ports (30000 -30031) to the corresponding ports as programmed here.



MGI Cards	IP	Start Port	Gateway	Netmask
Slots Select				
1-1	10.0.0.7	10000	10.0.0.1	255.255.255.0
1-2	10.0.0.8	15000	10.0.0.1	255.255.255.0
1-3	10.0.0.9	20000	10.0.0.1	255.255.255.0
1-4	10.0.0.10	25000	10.0.0.1	255.255.255.0
1-5				
2-1	10.0.0.11	35000	10.0.0.1	255.255.255.0
2-2	10.0.0.12	40000	10.0.0.1	255.255.255.0
2-3	10.0.0.13	45000	10.0.0.1	255.255.255.0
2-4	10.0.0.14	50000	10.0.0.1	255.255.255.0
2-5				

© SAMSUNG Telecommunications America, L.P.

IP Phone

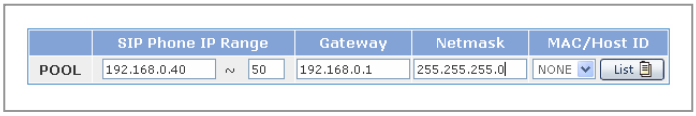
Allocate the IP range for the IP phone using DHCP mode. The DHCP IP pool allocated in this menu is set to authorize an IP phone of the ITP-5000 series to receive an IP address.

Item	Description
IP Range	IP range of IP phone(Maximum number of IP phone is 120) If one IP is entered, enter like '192.168.0.20~20'.
Gateway	Gateway data entered in the CALL Server item
Netmask	Netmask data entered in the CALL Server item
MAC/Host-ID	Client authentication type - NONE: Executes DHCP IP request without authentication. - MAC: Click the [List] button to enter MAC address of IP phone for authentication. - HOST: Uses HOST ID internally specified. Authorizes a phone of the ITP-5000 series.

© SAMSUNG Telecommunications America, L.P.

SIP Phone

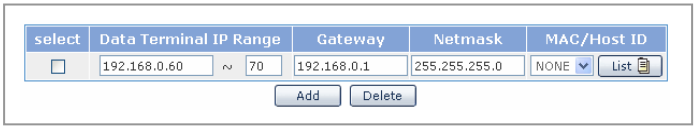
Allocate the IP range of standard SIP phone on the DHCP mode.



Item	Description
IP Range	IP range of SIP phone(Maximum number of IP phone is 120) If one IP is entered, enter like '192.168.0.40~40'.
Gateway	Gateway data entered in the CALL Server item
Netmask	Netmask data entered in the CALL Server item
MAC/Host-ID	Client authentication type - NONE: Executes DHCP IP request without authentication - MAC: Click the [List] button to enter MAC address of IP phone for authentication. - HOST: Since HOST ID internally specified is not used, click the [List] button to enter HOST ID.

Terminal

Allocate the IP range for the data terminals using DHCP.

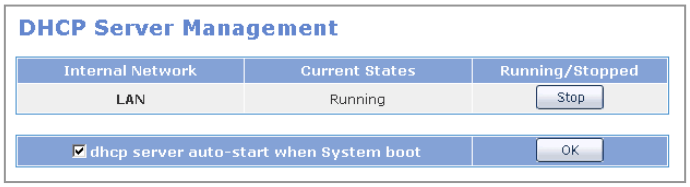


Item	Description
IP Range	IP range of data terminal(Maximum number of IP phone is 120) If one IP is entered, enter like '192.168.0.60~60'.
Gateway	Gateway data entered in the CALL Server item.
Netmask	Netmask data entered in the CALL Server item.
MAC/Host-ID	Client authentication type - NONE: Executes DHCP IP request without authentication. - HOST: Click the [List] button to enter HOST ID. - MAC: Click the [List] button to enter MAC address.

© SAMSUNG Telecommunications America, L.P.

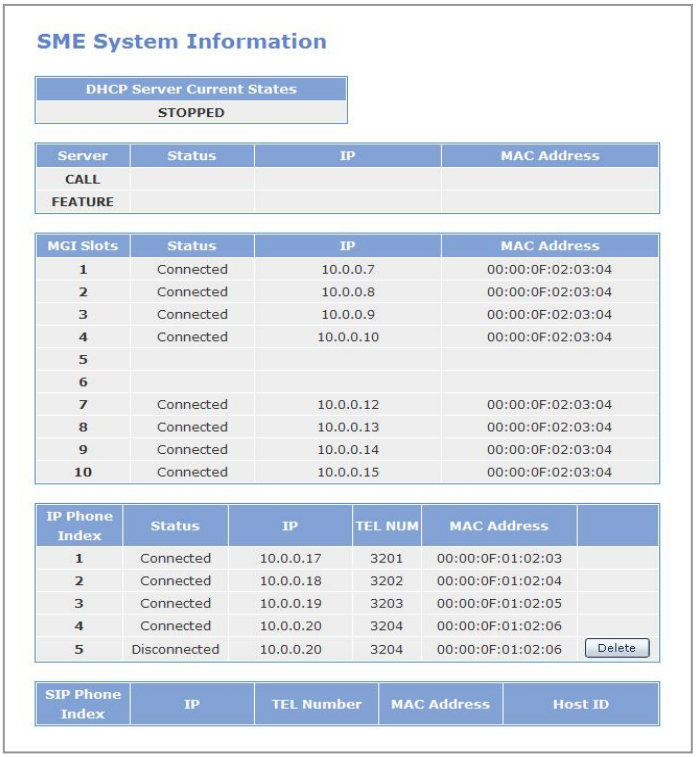
Management

Select the [DHCP Server] → [Management] menu to allow/disallow operating the DHCP Server. Check the 'Auto Start' item. Then, the service is provided automatically while the system reboots.



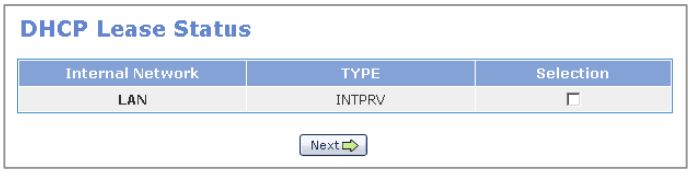
VoIP Status

Displays the OfficeServ 7200 systems VoIP status.



Leases Status

Select [DHCP Server] → [Leases Status] menus. Then, the IP address allocated by the DHCP Server to the data terminal will be displayed.

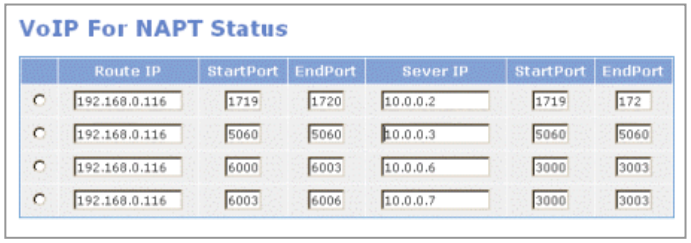


VoIP NAPT

OfficeServ 7200 Data Server NAPT service allows many private IP addresses to be multiplexed as a single public IP address and port. If the OfficeServ 7200 VoIP services provided by MCP and MGI use private IP, and they are connected behind the WIM router's public IP, DSMI will perform NAPT for signaling and media data packets for VoIP service. [VoIP NAPT] menu displays NAPT status for these VoIP communications.

Status

Display the NAPT status for the VoIP related services configured on the DSMI. The [Status] menu displays the service data of the external IP and port combination, and its corresponding internal IP and port combination.



© SAMSUNG Telecommunications America, L.P.

SIP ALG Menu

SIP ALG allows SIP (Session Initiation Protocol) software or hardware clients to setup, tear down, and pass voice and call control messages seamlessly through the OfficeServ 7200 NAT-enabled firewall.

Select [SIP ALG] to display the submenus of SIP ALG on the upper left section of the window.

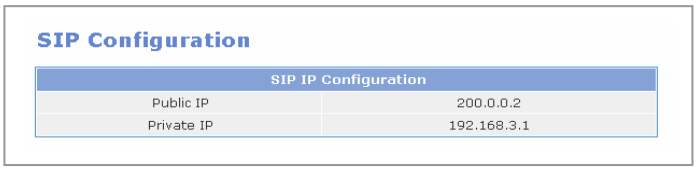
Menu	Description
Config	Sets SIP environment
Management	Allows/Disallows SIP ALG implementation. Set SIP ALG to be executed when the system reboots.

Config

Users are allowed to set the SIP environment on the [Config] menu. Set the following items and click the [Save] button.

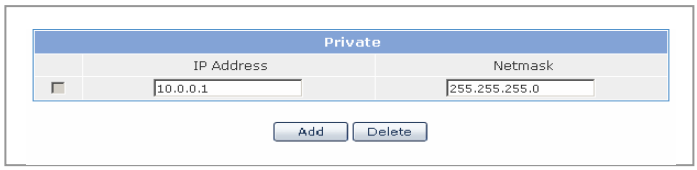
SIP Configuration

Displays firewall installation data.



Private

Enter the internal private IP area protected by the Data Server.

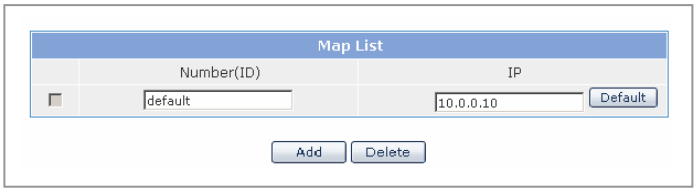


Click the [Add] button to additionally add private IP area inside of the firewall. The SIP device in the added private IP area provides ALG(SIP ALG) function. Set the target routing data directly or operate the target routing protocol to route to the added private IP area. Refer to Internal IP(LAN, DMZ) Setting on the [Firewall/Network] → [Management] → [Config] of this document for detailed information.

© SAMSUNG Telecommunications America, L.P.

Map List

Enter SIP devices data inside of the firewall.



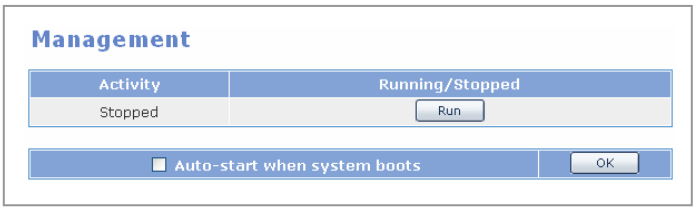
If an IP or phone number does not exit in the SIP message sent from the outside of a firewall, the SIP message is converted and sent to the IP terminal set in the ‘default’ item. Thus, enter the target value into this item. Since setting is convenient if all traffic is regarded as the calls of a digital phone through the Call Server, the IP of the Call Server should be entered in the ‘default’ item.

For example, in the window above, all station numbers except 3321 and 3322 is processed by the Call Server(10.0.0.100).

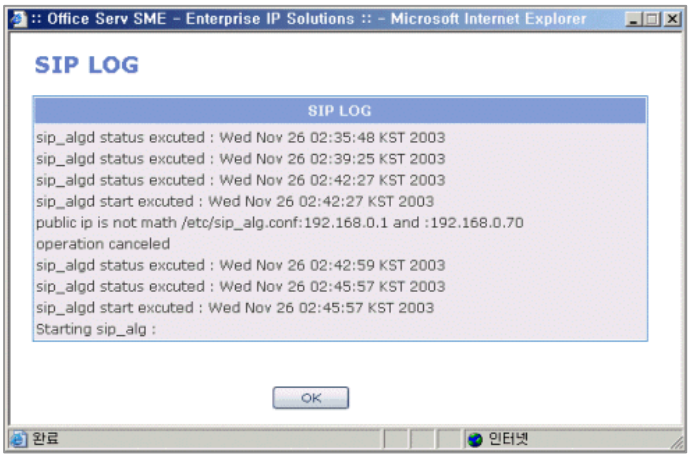
© SAMSUNG Telecommunications America, L.P.

Management

Select the [Management] menu to allow/inhibit operating SIP ALG. Check the 'Auto Start' item. Then, the service is provided automatically when the system reboots.



Click the [Run] button to operate the SIP ALG and the following window is displayed:

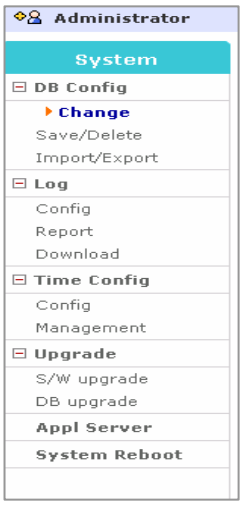

:: Office Serv SME - Enterprise IP Solutions :: - Microsoft Internet Explorer
SIP LOG
SIP LOG
sip_algd status excuted : Wed Nov 26 02:35:48 KST 2003
sip_algd status excuted : Wed Nov 26 02:39:25 KST 2003
sip_algd status excuted : Wed Nov 26 02:42:27 KST 2003
sip_algd start excuted : Wed Nov 26 02:42:27 KST 2003
public ip is not math /etc/sip_alg.conf:192.168.0.1 and :192.168.0.70
operation canceled
sip_algd status excuted : Wed Nov 26 02:42:59 KST 2003
sip_algd status excuted : Wed Nov 26 02:45:57 KST 2003
sip_algd start excuted : Wed Nov 26 02:45:57 KST 2003
Starting sip_alg :
OK
완료
인터넷

The window above displays when SIP ALG is executed normally. However, errors are found, the 'operation canceled' message is displayed.

© SAMSUNG Telecommunications America, L.P.

System Menu

Select [System] to display the submenus of System on the upper left section of the window.



Menu	Submenu	Description
DB Config	Change	Changes the operating DB to other saved or default DB.
	Save/Delete	Saves or deletes DB.
	Import/Export	Imports the DB to Admin terminal for backup or exports the DB from terminal for restore.
Log	Config	Sets type of logs to be recorded.
	Report	Searches logs according to type and time.
	Download	Downloads all log files to a local computer.
Time Config	Config	Sets Date and Time by SNTP or Manual.
	Management	Activates the connection to the configured SNTP server if SNTP is selected for the Time Configuration. Allows/disallows the SNTP service to auto start when systems boots.

© SAMSUNG Telecommunications America, L.P.

(Continued)

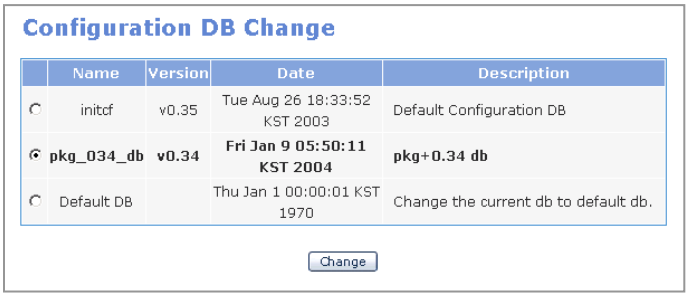
Menu	Submenu	Description
Upgrade	S/W upgrade	Upgrades DB package, Kernel, Ramdisk, and Application.
	DB upgrade	Upgrades DB to the latest package version.
Appl Server	-	Executes Telnet, FTP, and SSH services to connect to OfficeServ 7200 Data Server remotely.
Reboot	-	Reboots the system

DB Config

Users are allowed to save or delete DB, or to change the operating DB to other DB on the [DB Config] menu.

Change

Users are allowed to change the operating Database to other saved DB or default DB on the [Change] menu. The operating DB below is displayed with bold letters. Select the DB to be changed and click the [Change] button. Please note that changing the database will cause the system to restart.

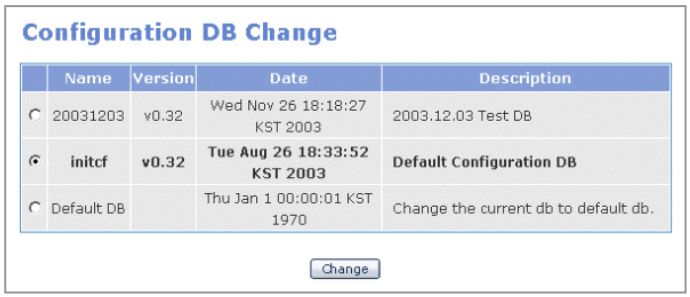


CAUTION

DB Change

The DBs of the WM module and LIM module are integrated in the OfficeServ 7200 Data Server. When the DB is changed, the system restarts.

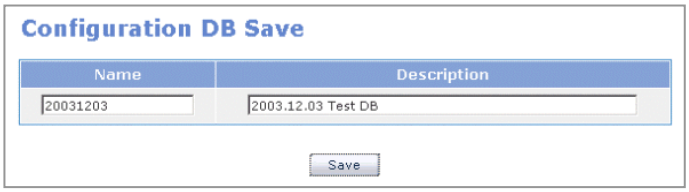
Select ‘Default DB’ and click the [Change] button. Then, initial DB is initialized and changed as shown below: initcf is the initial DB. When the Default DB is selected, the system is initialized. Thus, connect to the web manager through the LAN port(10.0.0.1) of the internal network.



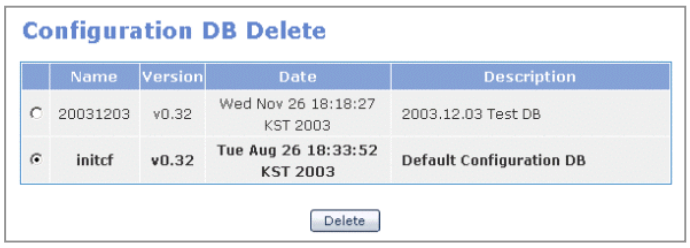
Save/Delete

Users are allowed to save the current operating DB, or delete the DB saved on the [Save/Delete] menu.

Enter the DB name and description and click the [Save] button to save the DB. Then, the saved DB is registered on the <Configuration DB Delete> window.



Select the DB to be deleted and click the [Delete] button. The running operating DB is displayed with bold letters and can not be deleted.



Import/Export

Users are allowed to import the DB to be backed up to the operating terminal on the [Import/Export] menu, or export the backup DB from a terminal.

Import

DB file should be saved in a terminal to import the DB. Enter the DB file location, or click the [Browse] button to select the target file, and click the [Import] button. Then, the DB is registered on the <Configuration DB Export> window.

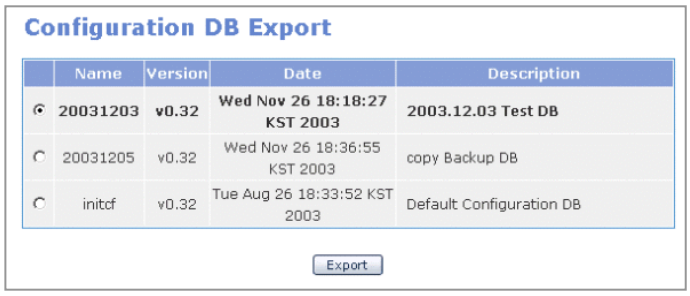
CHECK

If Errors are Found When [Import] is Executed, Check the Following Cases:

- Corresponding file does not exit after file location is entered
- Click the [Import] button without entering anything in the corresponding field.
- DBs whose names are identical
- File name is changed in the existing DB
- The first letter is left blank.

Export

The current DB set is displayed with bold letters. Select the target DB and click the [Export] button to save DB to the selected area of a terminal.



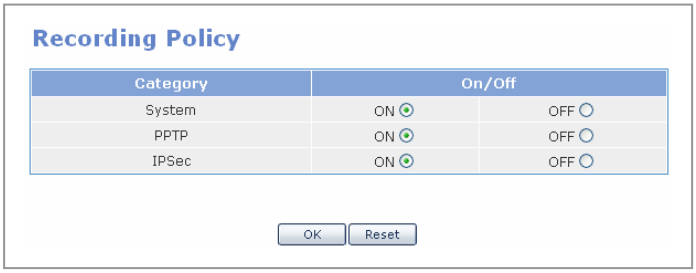
If the DB is sent to a terminal, click the [Save] button and download the DB.

Log

Users are allowed to search or download logs while logs are set to be recorded on the [Log] menu.

Config

Set logs to be recorded on the [Log Config] menu. Set the logs to be recorded to ‘On’, and otherwise, set to ‘Off’.

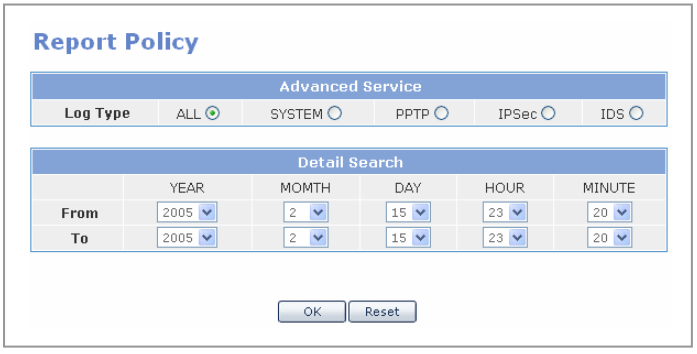


Log types are as follows:

- System log: System related log
- PPTP log: Log related with PPTP protocol of VPN
- IPSec log: Log related with IPSec protocol of VPN

Report

Search logs according to type and time on the [Log Report] menu.



- Log Type: Select the specific log type and search logs according to the type.
  - ALL: Search all logs
  - SYSTEM: Search all logs except PPTP, IPSec, and IDS logs
  - PPTP: Search logs of PPTP protocol of VPN
  - IPSec: Search logs of IPSec protocol of VPN
  - IDS: Search IDS protocol logs
- Detail Search: Enter the specific time and search logs according to the time.

© SAMSUNG Telecommunications America, L.P.

Select the type and time of logs, and click the [OK] button to display the window below:

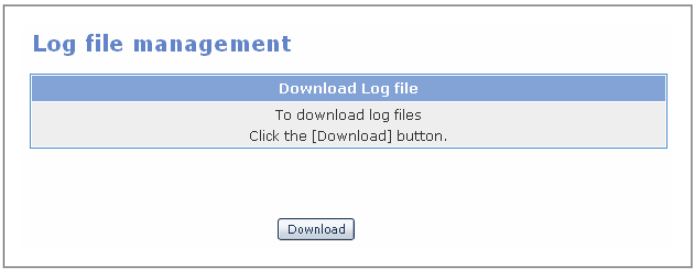
Log Report

Date/Time	Message	Type
2003/11/26 00:00:07	restart	syslogd
2003/11/26 00:00:08	syslogd startup succeeded	syslog
2003/11/26 00:00:08	klogd 1.4.1, log source = /proc/kmsg started.	kernel
2003/11/26 00:00:08	Cannot find map file.	kernel
2003/11/26 00:01:22	-- admin[313]: ROOT LOGIN ON ttyS/1	
2003/11/26 00:01:48	Received TERM or STOP signal... shutting down...	snmpd
2003/11/26 00:01:49	snmpd shutdown succeeded	snmpd
2003/11/26 00:01:49	snmpd startup succeeded	snmpd
2003/11/26 00:01:49	NET-SNMP version 5.0.8	snmpd
2003/11/26 00:01:59	[smux_accept] accepted fd 13 from 127.0.0.1:1027	snmpd
2003/11/26 00:01:59	accepted smux peer: oid iso.3.6.1.2.1.14, password ospfd, descr quagga-0.96.2	snmpd
2003/11/26 00:01:59	[smux_accept] accepted fd 14 from 127.0.0.1:1028	snmpd
2003/11/26 00:01:59	accepted smux peer: oid iso.3.6.1.2.1.23, password ripd, descr quagga-0.96.2	snmpd

First | Prev.+10 | Prev. | 1/9 | Next | Next+10 | Last

Download

Users are allowed to download all log files saved to a local computer on the [Log Download] menu.

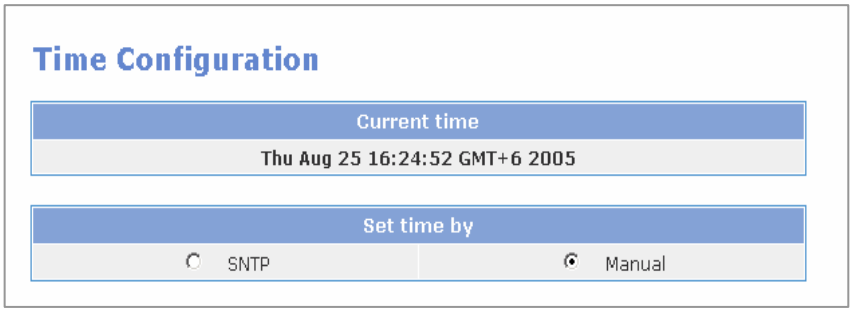


Time Config

The OfficeServ 7200 Data Server uses the time configuration to time stamp log events, and perform other activities for other internal purposes. Users are allowed to set the date and hour of the system on the [Time Config] menu.

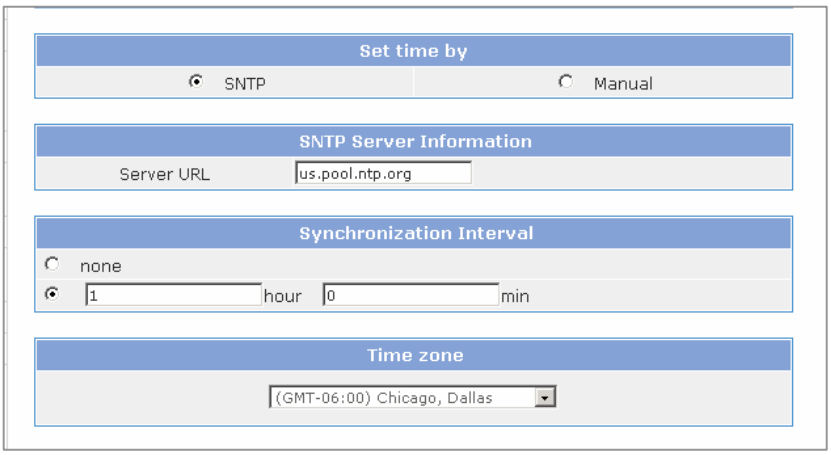
Config

Click [Time Config] → [Config] to set the local time using the SNTP (Simple Network Time Protocol) automatically or set the local time manually.



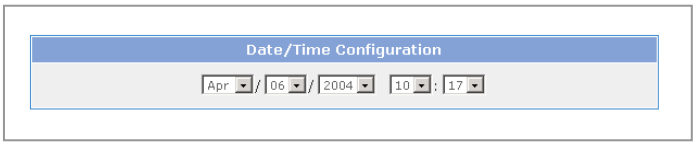
SNTP server

Select the SNTP server option. Then, the window below will appear. Register a server from which information on date and time will be imported and set the Synchronization Interval for the interval of time between each request the OS 7200 sends out to the time server. Then, click [OK].



Manual

Select the Manual option. Then, the window below will appear. Enter date and time manually and click [OK].



NOTE

System Time Information

Since Internal Real-Time Clock(RTC) does not exist in the Data Server system, the set time information is only saved every hour. Thus, when the system restarts, the time set in the past may be different.

Time zone

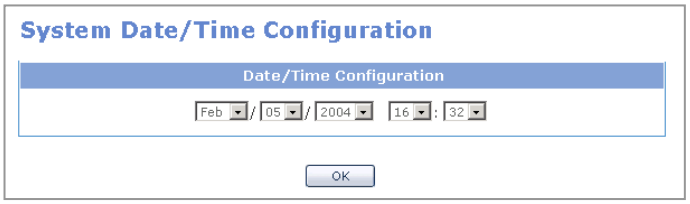
Set the time zone of the target area(city name). After the setting, click the [OK] button.

© SAMSUNG Telecommunications America, L.P.

Management

Select the [Time Config] → [Management] menu and set the time. If the system time is set by SNTP, select Time Setting to register and receive the date and hour from the configured SNTP server.

If the 'Auto Start' item is checked, the service is provided automatically when the system reboots.



Upgrade

Users are allowed to upgrade Kernel, Ramdisk, Application, and DB package on the [Upgrade] menu.

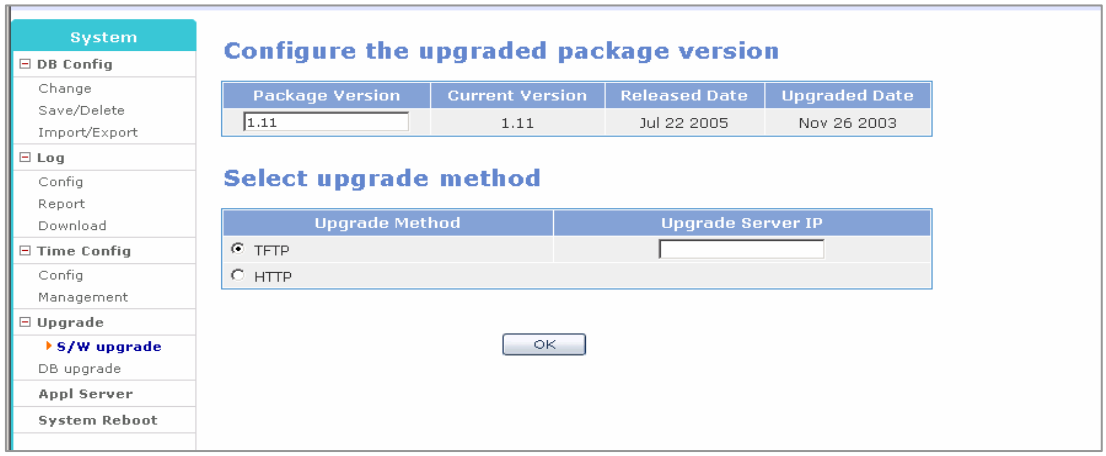
NOTE

'ds-pkg-vx.xx.tar.gz' File

This file is for the system upgrade used in [System] → [Upgrade] → [Package]. System DB maintains after this file is upgraded.

S/W Upgrade

Set the package version and upgrade method on the [Upgrade] → [S/W upgrade] menu. The upgrade methods are categorized into TFTP type and HTTP type.



Upgrade through TFTP

Users are allowed to upgrade the OfficeServ 7200 system using upgrade file on the TFTP server.

After entering the package version to be updated in the 'Package Version' field and select 'TFTP' server address, click the [OK] button. If the upgrade is successfully finished, reboot the OfficeServ 7200 system. Alarm message occurs when the upgrade server is not found or when errors are found during upgrade.

© SAMSUNG Telecommunications America, L.P.

Upgrade Through HTTP

Users are allowed to upgrade the OfficeServ 7200 system by uploading the upgrade file from a terminal where package file to be upgraded exists.

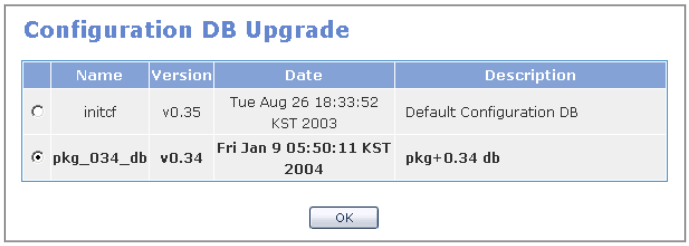
Enter the package version to be updated in the 'Package Version' field and click the 'HTTP' and click the [OK] button to display the window below:

Select the file to be uploaded of a terminal and click the [OK] button to upgrade. After the upgrade ends successfully, the OfficeServ 7200 system reboots.

DB Upgrade

Upgrade the DB to the latest on the [Upgrade] → [DB File] menu.

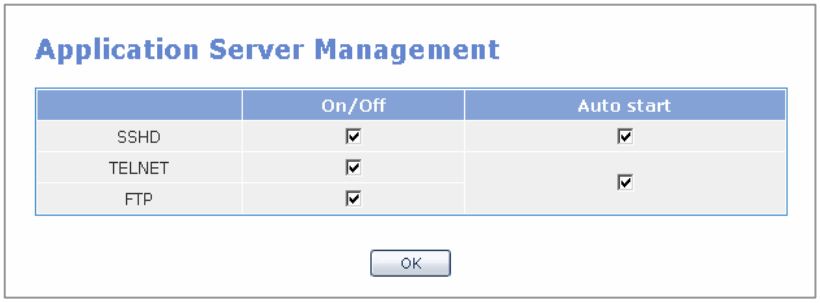
Select the DB to be upgraded and click the [OK] button to upgrade to the latest version. If the upgrade ends successfully, the Version item is changed into the latest version. However, if the upgrade does not end successfully, an alarm message is displayed.



© SAMSUNG Telecommunications America, L.P.

Appl Server

If the SSH, Telnet, and FTP services are selected on the [Appl Server] menu, the user can access the WIM board from a remote area. In addition, If the 'Auto Start' item is checked, the service is provided automatically when the system reboots.



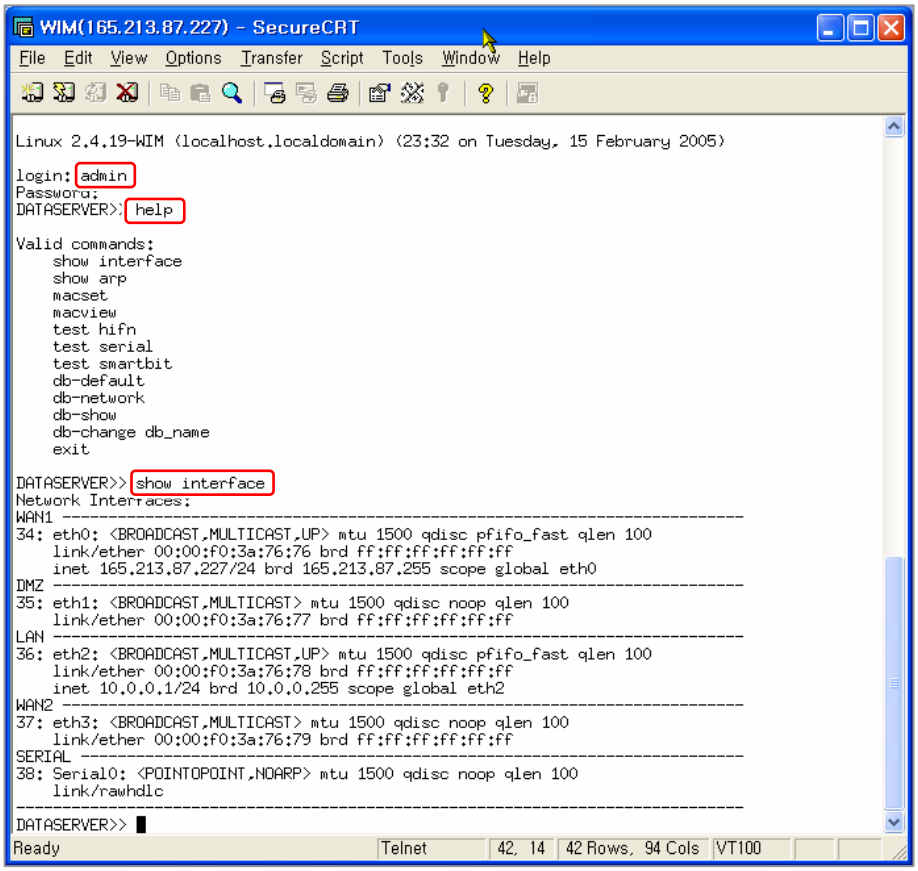
NOTE

Assigned Active Channel to 'Response Status'

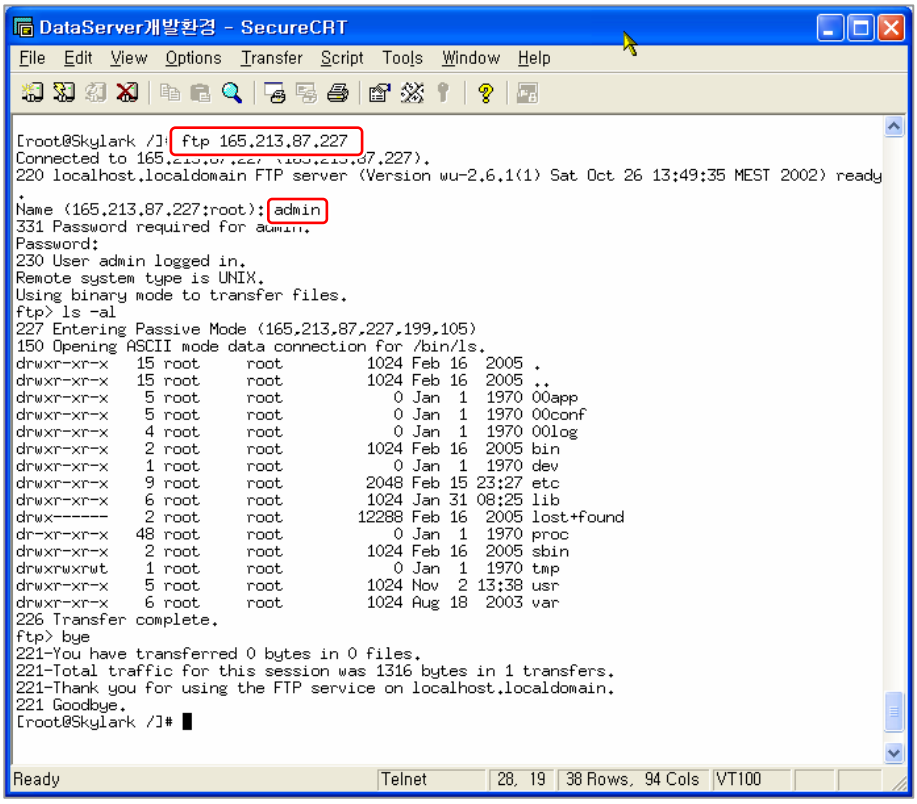
- SSH can be accessed regardless of external network or internal network.
- If a firewall is strengthened, accessing the system from an external network through Telnet/FTP is not available. For connection, release the target access firewall of the corresponding service port by selecting [Firewall/Network] → [Port ACL].
- Default administrator ID is set to 'admin', and password is set to 'admin'.

The connection methods through WAN and LAN IP by using Telnet, FTP, and SSH applications are as follows:

Connecting via Telnet



Connecting via FTP

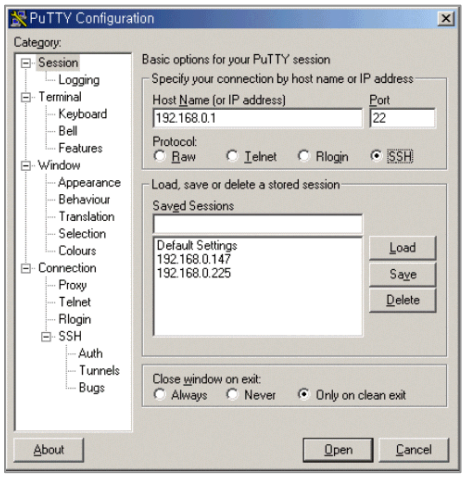

DataServer개발환경 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
[root@Skylark /]# ftp 165.213.87.227
Connected to 165.213.87.227 (165.213.87.227).
220 localhost.localdomain FTP server (Version wu-2.6.1(1) Sat Oct 26 13:49:35 MEST 2002) ready
.
Name (165.213.87.227:root): admin
331 Password required for admin.
Password:
230 User admin logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
227 Entering Passive Mode (165,213,87,227,199,105)
150 Opening ASCII mode data connection for /bin/ls.
drwxr-xr-x 15 root root 1024 Feb 16 2005 .
drwxr-xr-x 15 root root 1024 Feb 16 2005 ..
drwxr-xr-x 5 root root 0 Jan 1 1970 00app
drwxr-xr-x 5 root root 0 Jan 1 1970 00conf
drwxr-xr-x 4 root root 0 Jan 1 1970 00log
drwxr-xr-x 2 root root 1024 Feb 16 2005 bin
drwxr-xr-x 1 root root 0 Jan 1 1970 dev
drwxr-xr-x 9 root root 2048 Feb 15 23:27 etc
drwxr-xr-x 6 root root 1024 Jan 31 08:25 lib
drwx------ 2 root root 12288 Feb 16 2005 lost+found
dr-xr-xr-x 48 root root 0 Jan 1 1970 proc
drwxr-xr-x 2 root root 1024 Feb 16 2005 sbin
drwxrwxrwt 1 root root 0 Jan 1 1970 tmp
drwxr-xr-x 5 root root 1024 Nov 2 13:38 usr
drwxr-xr-x 6 root root 1024 Aug 18 2003 var
226 Transfer complete.
ftp> bye
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 1316 bytes in 1 transfers.
221-Thank you for using the FTP service on localhost.localdomain.
221 Goodbye.
[root@Skylark /]#
Ready
Telnet
28, 19
38 Rows, 94 Cols
VT100

Connecting via SSH

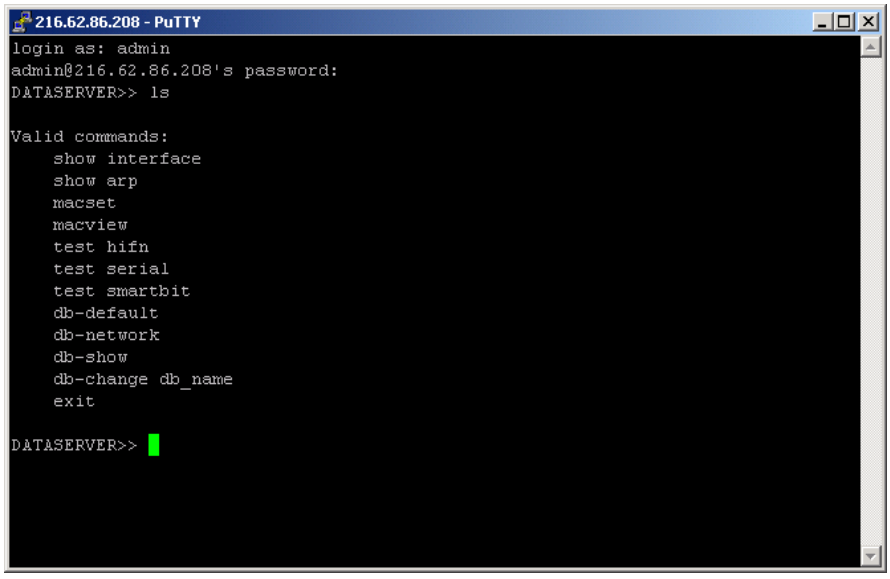
OfficeServ 7200 supports SSH, Secure Shell, allowing secure access to the Command Line Interface via an encrypted path between the system and the management station. SSH uses a client/server architecture. A public or commercially available SSH client is required to be installed on the Admin terminal. The example shown below uses SSH connection client Putty. The procedure for installing the Putty program and executing the SSH connection program is as follows:

1. Visit the web site below and download the Putty package: 'http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html'

2. Execute the 'putty.exe' file. The window below is displayed. Enter the firewall address in the Host Name field and select [Open].



3. Then, the window below is displayed. Enter the login ID and password.



Reboot

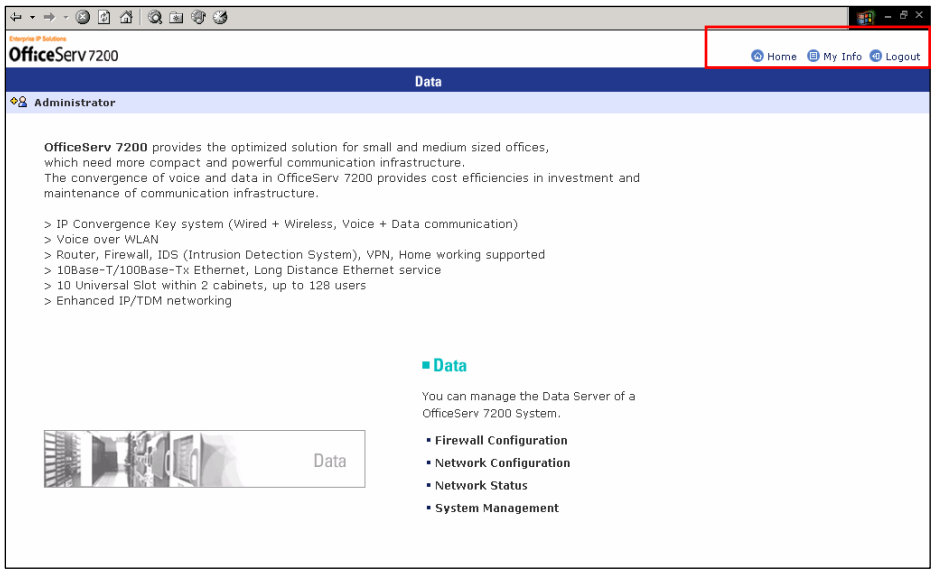
Users are allowed to reboot the system on the [Reboot] menu.

If the [OK] button is clicked, all services ends and the system reboots.
Then, since the Data Server web screen does not operate until the network and services start to be executed, close the web screen and reconnect the system.

© SAMSUNG Telecommunications America, L.P.

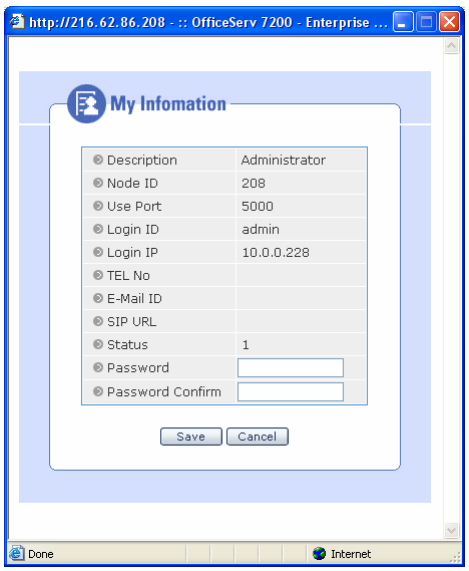
Home, My Info & Logout

Menus are found in the upper right corner of the web-based management window after logging into the Data Server management.


OfficeServ 7200
Home
My Info
Logout
Data
Administrator
OfficeServ 7200 provides the optimized solution for small and medium sized offices, which need more compact and powerful communication infrastructure. The convergence of voice and data in OfficeServ 7200 provides cost efficiencies in investment and maintenance of communication infrastructure.
> IP Convergence Key system (Wired + Wireless, Voice + Data communication)
> Voice over WLAN
> Router, Firewall, IDS (Intrusion Detection System), VPN, Home working supported
> 10Base-T/100Base-Tx Ethernet, Long Distance Ethernet service
> 10 Universal Slot within 2 cabinets, up to 128 users
> Enhanced IP/TDM networking
Data
You can manage the Data Server of a OfficeServ 7200 System.
Data
Firewall Configuration
Network Configuration
Network Status
System Management

The navigation menu contains the following three menus:

- Home – Home menu brings the user back to the OfficeServ 7200 Data introduction page.
- My Info – My Information page provides the Administrator's log in ID and IP. The administrator login password can also be changed under this menu.



- Logout – Logout menu logs the administrator out.

ANNEX A. VPN Setting in Windows XP/2000

If IPSec and PPTP should be set on the [VPN] menu of the OfficeServ 7200 Data Server, VPN client should be also set on the MS Windows. This section describes how to set VPN on the Windows XP. The Windows 2000 case is similar with the Windows XP case.

Under the following network environment, the setting procedures of IPSec and PPTP are as follows:

- External IP address of the OfficeServ: 211.217.127.40
- Internal IP address of the OfficeServ: 192.168.0.1
- Internal network IP address: 192.168.0.0
- Internal network Netmask: 255.255.255.0
- IP address of a Windows XP/2000-installed client PC: 211.217.127.73

IPSec Setting

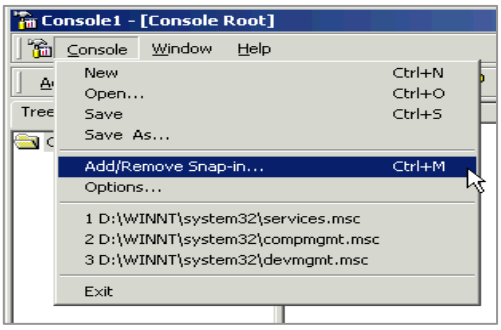
IPSec and various encryption/authentication algorithms can be used through the installation CD and Windows update in Windows XP/2000. Additionally, LAN to VPN client can be configured through the IPSec.

IPSec Setting in Windows XP/2000

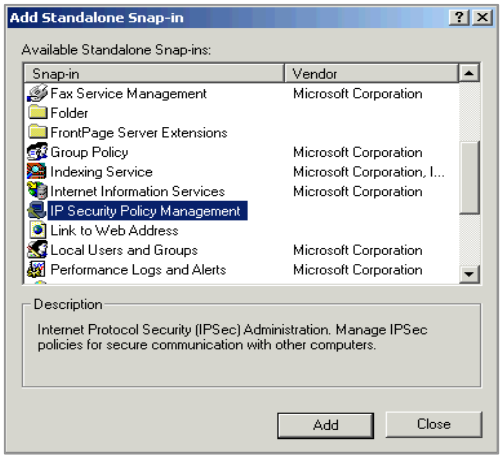
- Windows XP: Executes 'IPSeccmd.exe'in the Support/Tools setup folder of the Windows XP installation CD.
- Windows 2000: Download and install 'Windows 2000 Service pack 2'in the Windows update site. Or, execute 'IPSecpol.exe'in the Support/Tools setup in the Windows 2000 installation CD.

© SAMSUNG Telecommunications America, L.P.

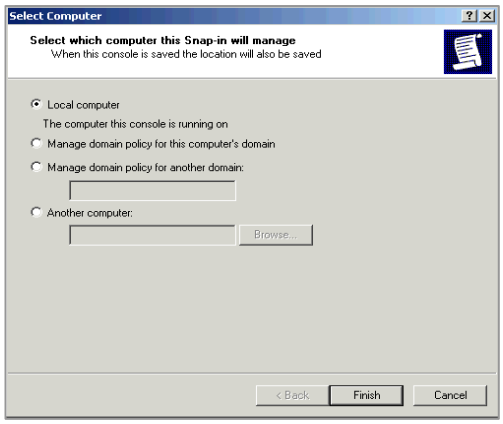
1. Select the [Start] → [Run] in the task bar and execute 'mmc' to display the window below: In the console window, select the [File] → [Add/Remove Snap-in…].



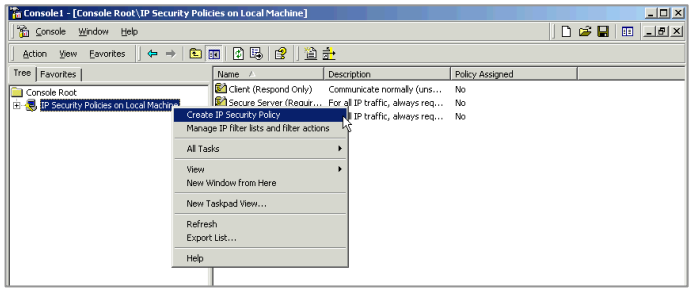
2. In the <Add/Remove Snap-in…>, click [Add] to display the following window: Select 'IP security policy management' in the Add/Remove Snap-in… menu and click [Add].



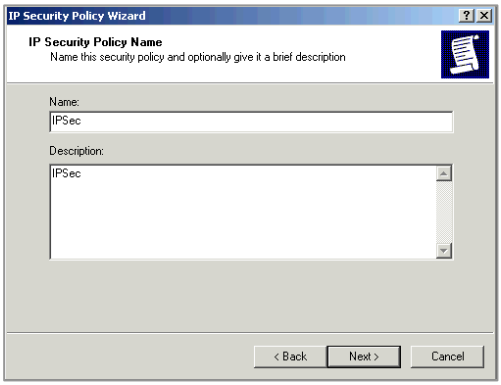
3. Select 'Local computer(T)'in the window below and click [Finish].


Select Computer
Select which computer this Snap-in will manage
When this console is saved the location will also be saved
Local computer
The computer this console is running on
Manage domain policy for this computer's domain
Manage domain policy for another domain:
Another computer:
Browse...
< Back
Finish
Cancel

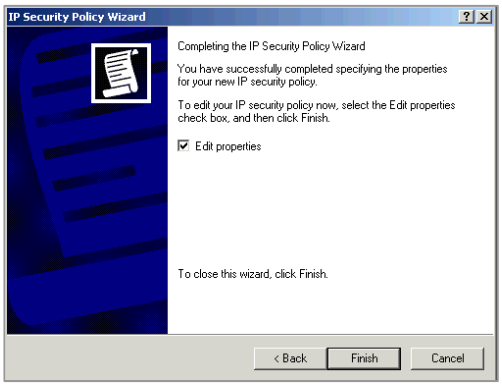
4. Move to the <Console> window. Then, 'IP Security Policies on Local Machine' of the 'Console Root' is created. Select the item and right click the [Create IP Security Policy] menu.


Console1 - [Console Root\IP Security Policies on Local Machine]
Console Window Help
Action View Favorites
Tree Favorites
Console Root
IP Security Policies on Local Machine
Name Description Policy Assigned
Client (Respond Only) Communicate normally (uns... No
Secure Server (Requir... For all IP traffic, always req... No
IP traffic, always req... No
Create IP Security Policy
Manage IP filter lists and filter actions
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help

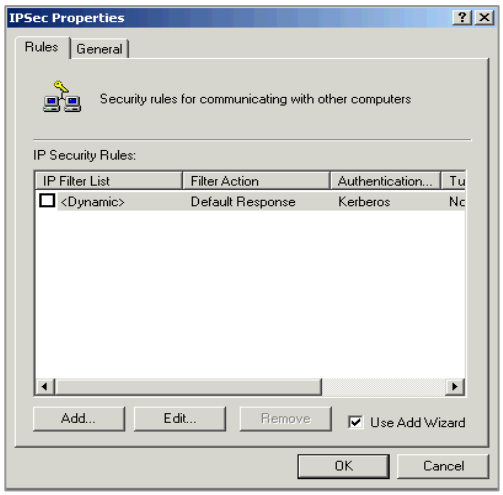
5. Click [Next] on the <IP Security Policy Wizard> window to display the window below: Enter the Name and Description and click [Next].



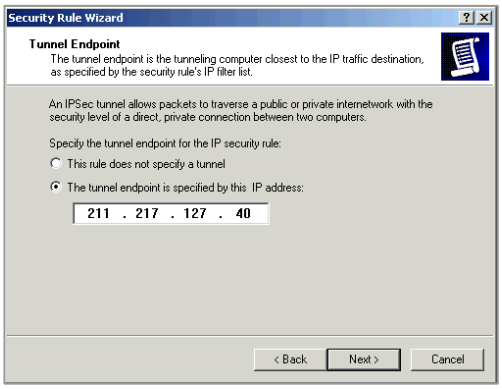
6. If 'Activate the default response rule(R)' is checked, release the check and click [Add] to display the window below: Check 'Edit Properties(P)' and click [Finish].


IP Security Policy Wizard
Completing the IP Security Policy Wizard
You have successfully completed specifying the properties for your new IP security policy.
To edit your IP security policy now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

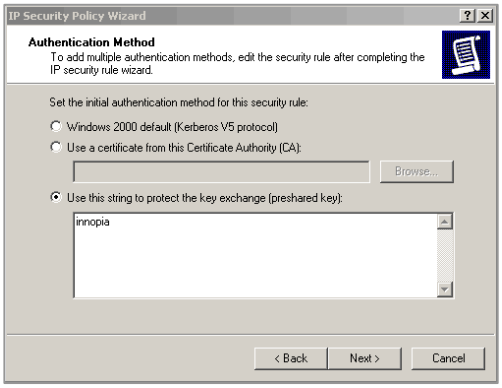
7. When the <XP_OPSec Registration Information> window is displayed, the created items are displayed. If the corresponding item is checked, release the check and click [Add].



8. Click [Add] on the <Security Rule Wizard> window to display the window below: Select 'The funnel endpoint is specified by this IP address' and enter the fire wall external IP address(211.217.127.40). Click [Next].

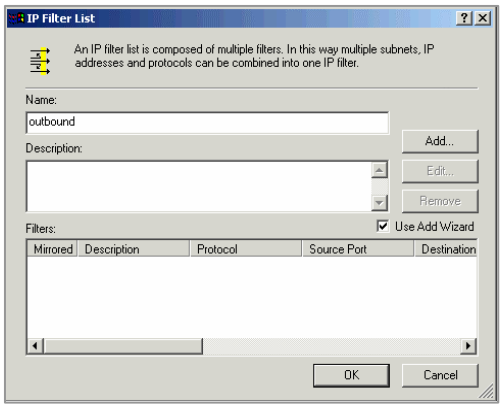

Security Rule Wizard
Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.
Specify the tunnel endpoint for the IP security rule:
This rule does not specify a tunnel
The tunnel endpoint is specified by this IP address:
211 . 217 . 127 . 40
< Back
Next >
Cancel

9. Select the Local Area Network(LAN) on the <Network Type> window and click [Add] to display the window below: Select 'Use this string to protect the key exchange [preshared key]' and enter the password registered with the firewall. Click [Next].

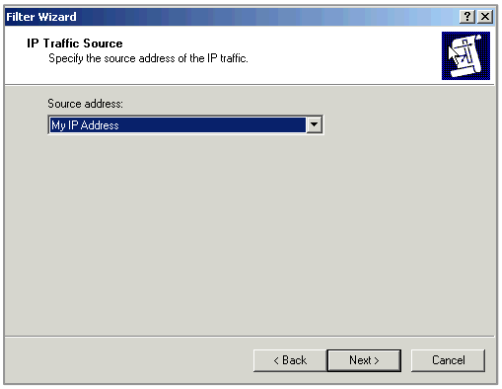

IP Security Policy Wizard
Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.
Set the initial authentication method for this security rule:
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this Certificate Authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
innopia
< Back
Next >
Cancel

© SAMSUNG Telecommunications America, L.P.

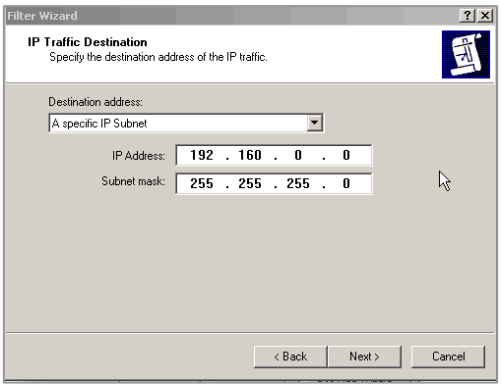
10. Click [Add] on the <Security Rule Wizard> window to display the window below: Enter 'outbound' in the Name field and click [Add].



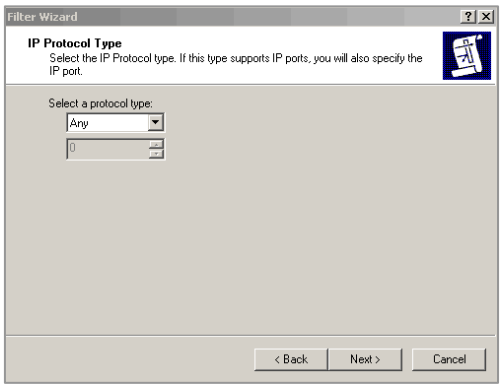
11. Click [Add] on the <IP Filer Wizard> window to display the window below: Select 'My IP address' in the Source address field and click [Add].



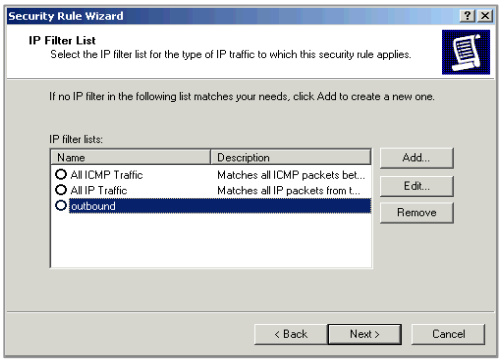
12. Select 'Specific IP Subnet' in the target address and enter the internal network address(192.168.0.0) and subnet mask(255.255.255.0). Click [Next].



13. Select 'All' from the protocol type selection and click [Add]. Check 'Edit Properties(P)' on the <IP Filter Wizard> window and click [Finish].

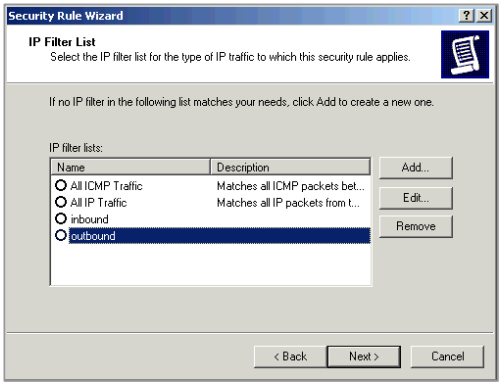

Filter Wizard
IP Protocol Type
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.
Select a protocol type:
Any
0
< Back
Next >
Cancel

14. Click [OK]. Then, the outbound item is created. Click [Add] to create the inbound item.

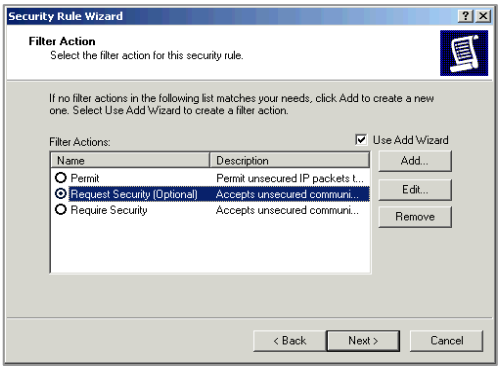

Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
outbound
Add...
Edit...
Remove
< Back
Next >
Cancel

15. Enter the 'inbound' in the Name field and click [Add] like step **10**. The above steps **11** through **13** also apply to this procedure.

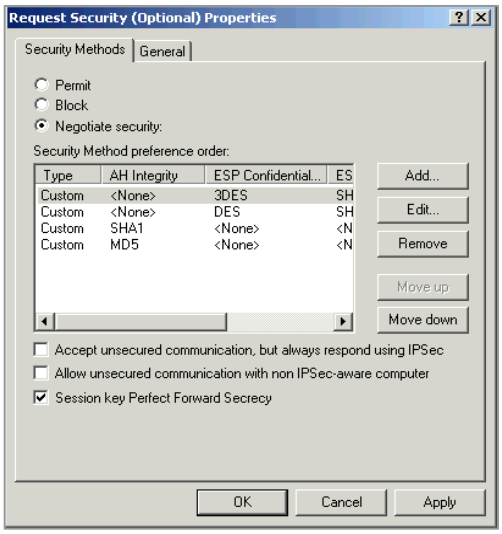
16. Click [Add] to display the window below: Then, select the 'outbound' item and click [Next].


Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
inbound
outbound
Add...
Edit...
Remove
< Back
Next >
Cancel

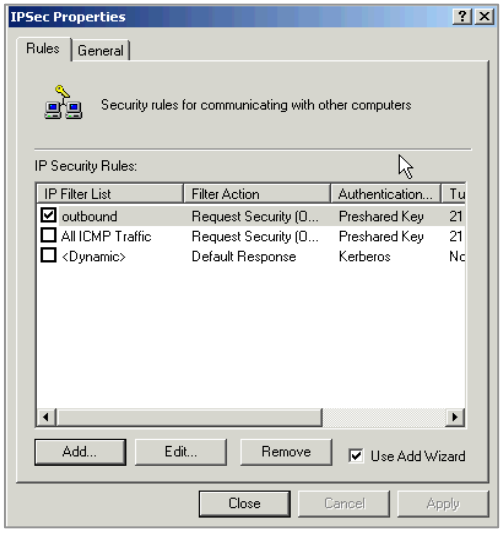
17. Select the 'Request Security [Optional]' item and click [Edit].



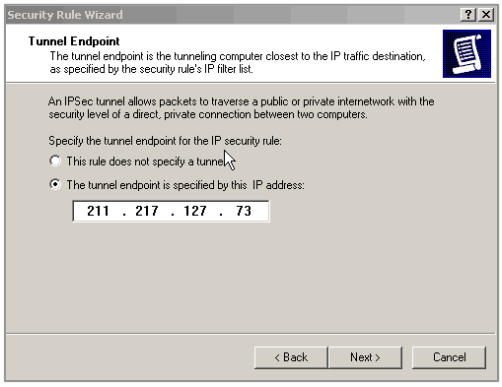
18. Select 'Negotiate security' and select 'AH Integrity(None), ESP Confidential(3DES), ESP Integrity(MD5)' in the Security Method preference order. Click [Move up] to move to the first row of the corresponding item. Check 'Session key Perfect Forward Secrecy(PFS)' and click [OK].



19. Check 'Edit Properties' and click [Finish] to display the window creating the outbound item. Click [Add] to create the inbound item.



20. Click [Next] on the <Security Rule Wizard> window to display the window below: Check 'The tunnel endpoint is specified by this IP address' and enter the IP address of a client PC. Click [Next].

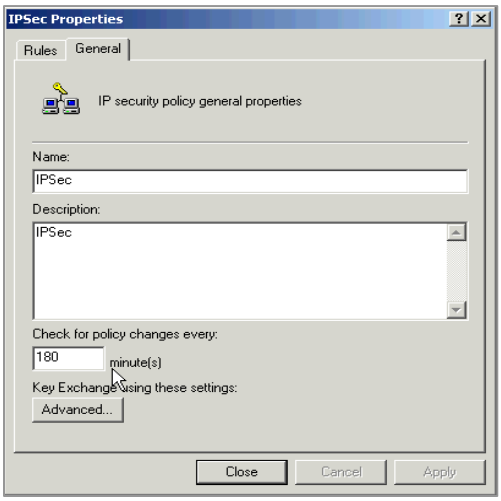

Security Rule Wizard
Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.
Specify the tunnel endpoint for the IP security rule:
This rule does not specify a tunnel
The tunnel endpoint is specified by this IP address:
211 . 217 . 127 . 73
< Back
Next >
Cancel

21. Select Local Area Network(LAN) on the <Network type> window and click [Next]. Select 'Use this string to protect the key exchange [preshared key]' and enter the password registered with the firewall. Click [Next].(Refer to step **9.**)

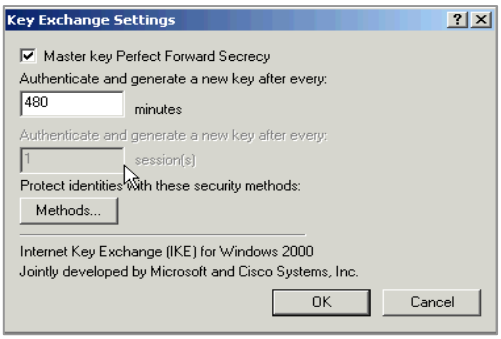
© SAMSUNG Telecommunications America, L.P.

22. Select the 'inbound' item in the step **16** window and click [Next]. Follow the step **17** and **18**.

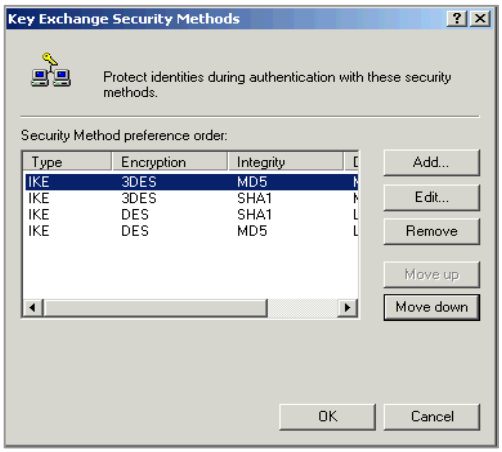
23. Check 'Edit Properties' and click [Finish] to display the window below: Select the [General] tab and click [Advanced].



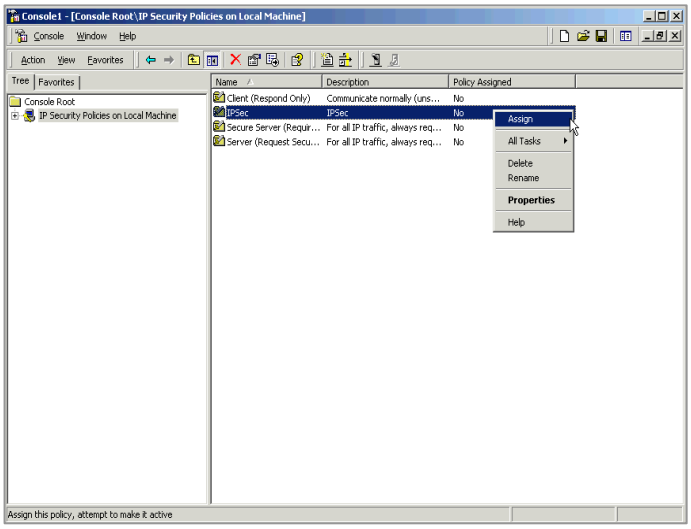
24. Check 'Master key Perfect Forward Secrecy(PFS)' and click [Methods…] in the window below:



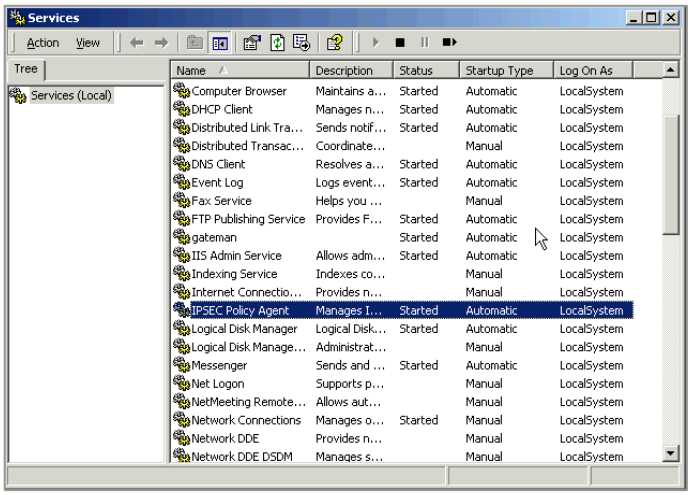
25. Select ‘Encryption(3DES), Integrity(MD5), Diffie-Hellman(Med)’ in the window below and click [Move up] to move the first row of the corresponding item. Click [OK].



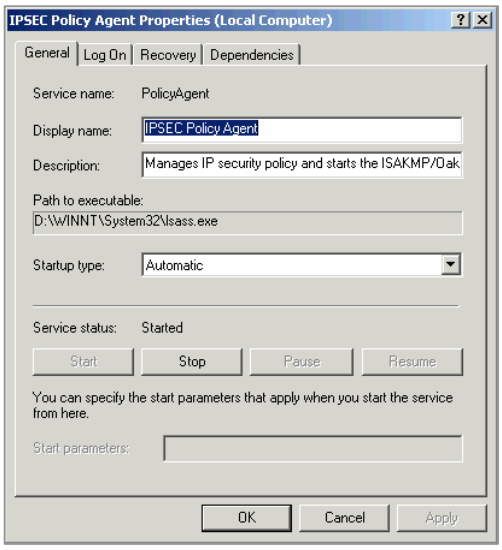
26. Select IP Security Policies on Local Machine’ on the <Console> window. Select the item newly created on the right corner of the window and right-click the [Assign] menu. Then, policy assignment is changed into ‘Yes’.



27. Select [Start] → [Program] → [Administrative Tools] → [Services] in the Window task bar and double click the 'IPSec Services' item.


Services
Action View
Tree
Services (Local)
Name Description Status Startup Type Log On As
Computer Browser Maintains a... Started Automatic LocalSystem
DHCP Client Manages n... Started Automatic LocalSystem
Distributed Link Tra... Sends notif... Started Automatic LocalSystem
Distributed Transac... Coordinate... Manual LocalSystem
DNS Client Resolves a... Started Automatic LocalSystem
Event Log Logs event... Started Automatic LocalSystem
Fax Service Helps you ... Manual LocalSystem
FTP Publishing Service Provides F... Started Automatic LocalSystem
gateman Started Automatic LocalSystem
IIS Admin Service Allows adm... Started Automatic LocalSystem
Indexing Service Indexes co... Manual LocalSystem
Internet Connectio... Provides n... Manual LocalSystem
IPSEC Policy Agent Manages I... Started Automatic LocalSystem
Logical Disk Manager Logical Disk... Started Automatic LocalSystem
Logical Disk Manage... Administrat... Manual LocalSystem
Messenger Sends and ... Started Automatic LocalSystem
Net Logon Supports p... Manual LocalSystem
NetMeeting Remote... Allows aut... Manual LocalSystem
Network Connections Manages o... Started Manual LocalSystem
Network DDE Provides n... Manual LocalSystem
Network DDE DSDM Manages s... Manual LocalSystem

28. Click [Stop] and click [Start] to restart the service in the window below:


IPSEC Policy Agent Properties (Local Computer)
General Log On Recovery Dependencies
Service name: PolicyAgent
Display name: IPSEC Policy Agent
Description: Manages IP security policy and starts the ISAKMP/Oak
Path to executable:
D:\WINNT\System32\lsass.exe
Startup type: Automatic
Service status: Started
Start Stop Pause Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK Cancel Apply

29. Verify the connection status of the firewall internal IP address through the ping command at a command prompt. If responses like the window below are displayed, the IP address is properly connected.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Negotiating IP Security.
Reply from 192.168.0.1: bytes=32 time=5 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=6 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4 ms TTL=255

Ping statistics for 192.168.0.1:
     Packets: Sent = 4, Received = 3, Lost = 1 <25% loss>.
Approximate round trip times in milli-seconds:
     Minimum = 4 ms, Maximum = 6 ms, Average = 5 ms
```

© SAMSUNG Telecommunications America, L.P.

PPTP Setting

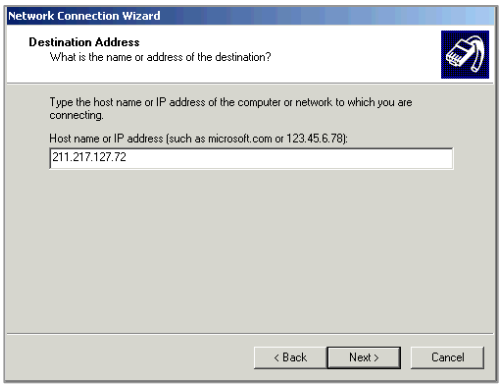
Users are allowed to configure VPN with PPTP by using the installation CD and through Windows update in Windows XP/2000.

> CAUTION
>
> **PPTP Setting in Windows XP/2000**
>
> In Windows XP/2000, the user can use DHCP client. If VPN PPTP client is connected while the DHCP client is operating, errors will be found. To prevent this problem, close the DHCP client operation on the [Start] → [Program] → [Administrative Tools] → [Services] menu of the Windows PPTP client installed.

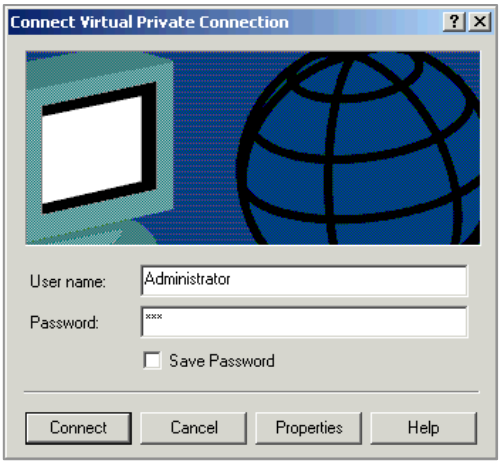
1. Double click the [My Network Environment] icon and select the [Property] item from the Windows desktop. Double click [Create New Connection] on the upper right corner of the screen to display the window below: Click [Next].

Network Connection Wizard
Welcome to the Network Connection Wizard
Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.
To continue, click Next.
< Back
Next >
Cancel

2. Select 'Connect to the network at my workplace' and click [Next] button to select 'Virtual Private Connection'. Click [Next] to display the window below: Enter the Host name or IP address and click [Next]. Enter the firewall external IP address and click [Finish] button.


Network Connection Wizard
Destination Address
What is the name or address of the destination?
Type the host name or IP address of the computer or network to which you are connecting.
Host name or IP address (such as microsoft.com or 123.45.6.78):
211.217.127.72
< Back
Next >
Cancel

3. Select [Start] → [Set] → [Network Connections] in the Windows task bar and select the host name entered in the window above to display the login window below: Enter the User name and Password to check if the VPN in a client is properly connected. Or, use the ping command like the **step 29** of 'IPSec Setting' to check the connection status.



After checking the VPN connection status, check if the shared directory of the internal computer connected to VPN can be accessed.

OfficeServ 7200 Data Server Quick Setup Guide: Network, Firewall & DHCP

This Quick Setup Guide is designed to provide you with basic setup procedures of configuring your OfficeServ 7200 Data Server WAN1 port connecting to a DLS, Cable Modem or T1 for office wide Internet access sharing.

This Guide will also cover the basic setup for the followings:

- NAT (Network Address translation): NAT translates IP address of your local area network to your public IP address for the Internet.
- Firewall and Packet Filtering: OS 7200 stateful packet inspection firewall features include DoS protection, blocking unwanted traffic from the Internet to your LAN, and blocking access from your LAN to Internet locations or services that you specify as off-limits.
- Port Forwarding with NAT: Although NAT prevents Internet users from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request.
- Data Server Access Control List: A list of hosts and/or networks permitted to access the ports and services on the OS 7200.
- DHCP (Dynamic Host Configuration Protocol): OS 7200 dynamically assigns network configuration information to attached PCs or network devices on the LAN using DHCP.

Before Setting Up Data Server

1. Power off all the hardware, including OS 7200, PCs, and cable or DSL modem.
2. Install the WIM board in OfficeServ 7200 Slot 1 and the LIM board in Slot 2. JP1, 2, 3, 4 of WIM should be installed toward the system back-board to ensure that WIM and LIM can be connected through the back panal. If JP1, 2, 3, 4 are installed in reverse direction, use an external Ethernet cable to connect between LAN port on the WIM module and one of the ethernet port on the LIM module.
3. Connect the LAN port of your PC to any of the 16 Ethernet port on the front of the LIM module by Ethernet cable. Repeat this step to connect more PCs or other network devices to the LIM module.
4. Connect your cable or DSL modem's Ethernet cable to WAN1 port of the WIM module.
5. Power on the cable or DSL modem, OfficeServ 7200, your PC and other network device(s).
6. Configure your PC IP address to 10.0.0.100, with subnet mask of 255.255.255.0 and gateway address of 10.0.0.1. Execute Internet Explore in your PC and enter the default management IP address 10.0.0.1 in the IP address window to connect to the system through Web. It is advisable to use Internet Explorer Version 6.0 or higher.

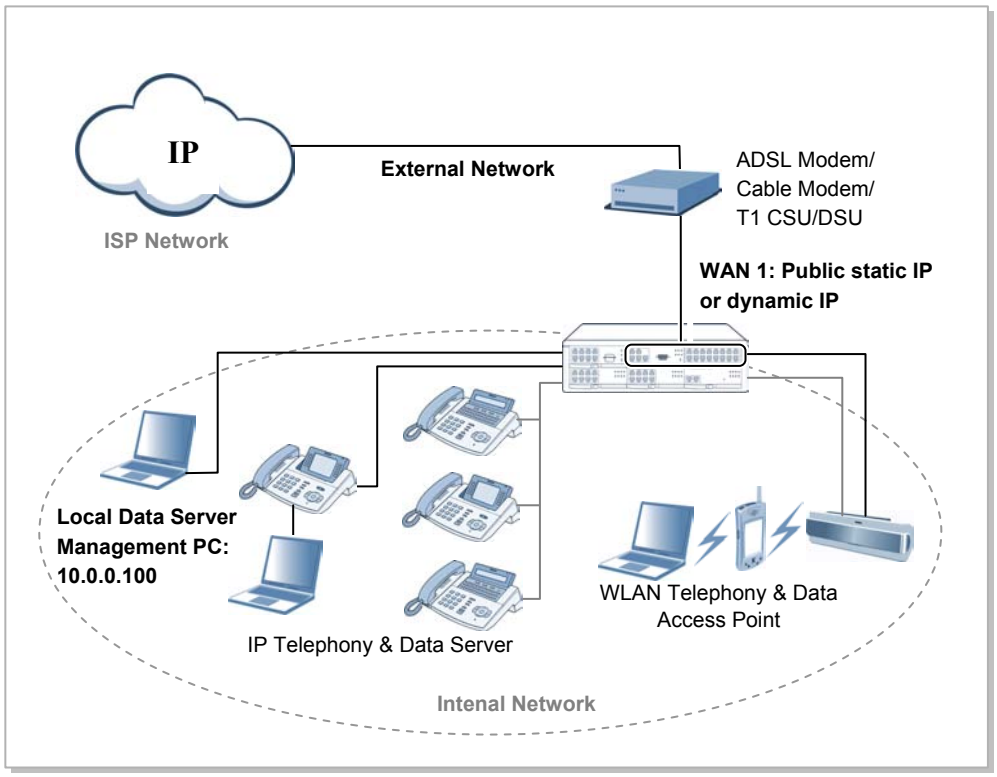
© Samsung Telecommunications America, L.P.

7. Once the following window appears, enter the Login ID and Password. Default ID and Password are 'admin''admin'.

Overview

Configure the WAN1 interface using a static public IP or a dynamic public IP and set the LAN port as an internal private network:

- Set WAN1 port to an external public IP (e.g., ADSL static IP Service or T1 with static IP connecting via external CSU/DSU).
- Set the LAN port to private network of 10.0.0.0/24.
- Set the PC IP to the private network IP (e.g., 10.0.0.100).



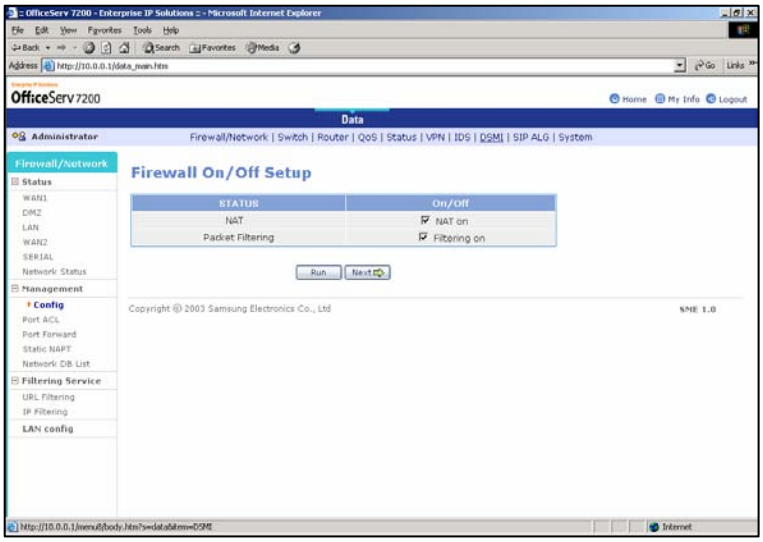
© Samsung Telecommunications America, L.P.

Setting Data Server

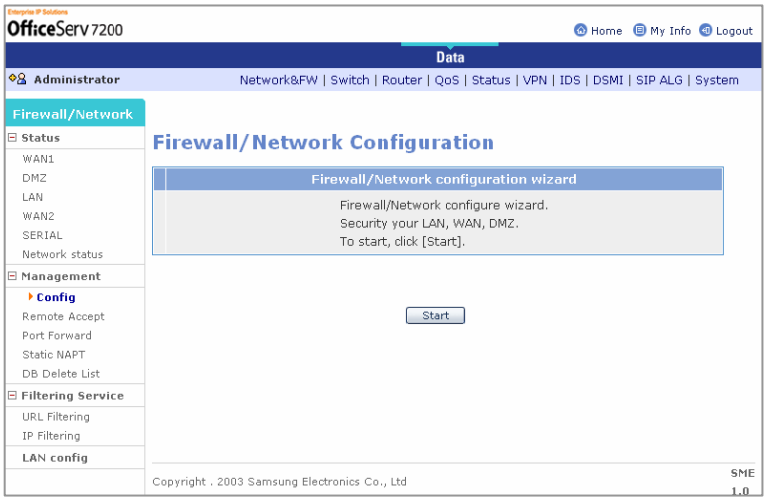
1. Select the [Firewall/Network] → [Management] → [Config] menu.

2. Check the 'NAT' and 'Packet Filtering' items to enable these functionalities, and click the [Run] button to start the configuration.

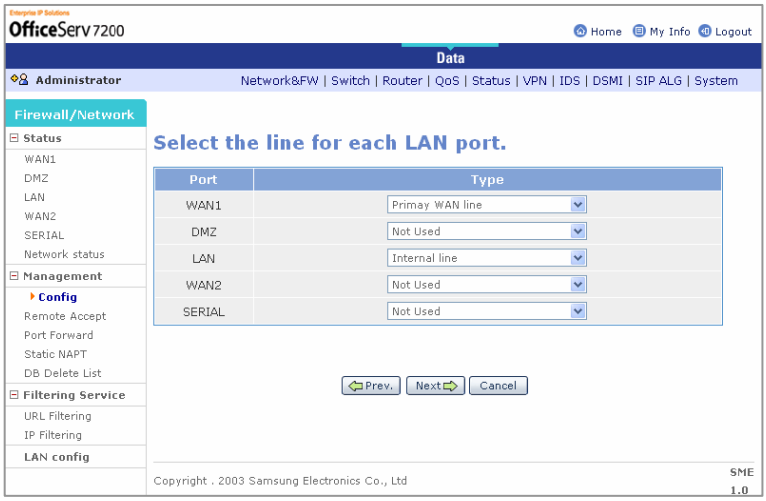
   Click the [Next] button to move to the next step.



3. Click the [Start] button to perform the Firewall/Network function.



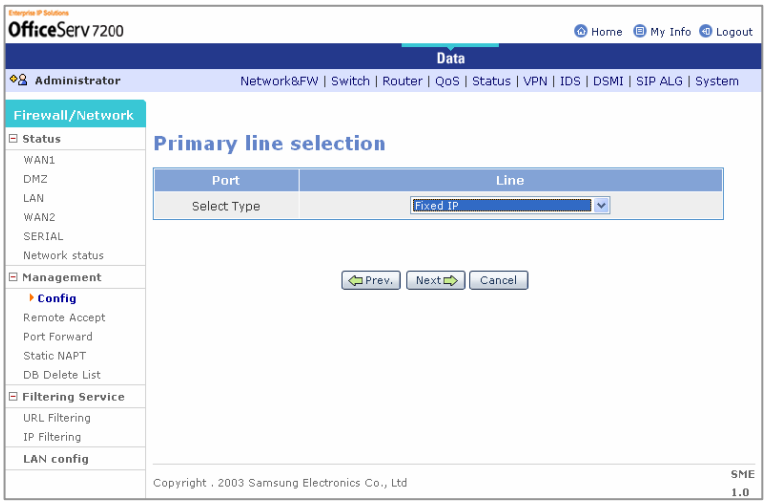
4. In this Quick Setup Guide, we will only use WAN1 for internet connection and LAN port to manage your private local network. So set the WAN1 port to 'Primary WAN Line' and the LAN port to 'Internal Line'. Click the [Next] button to move to the next step.



5. Set the Primary Line Type

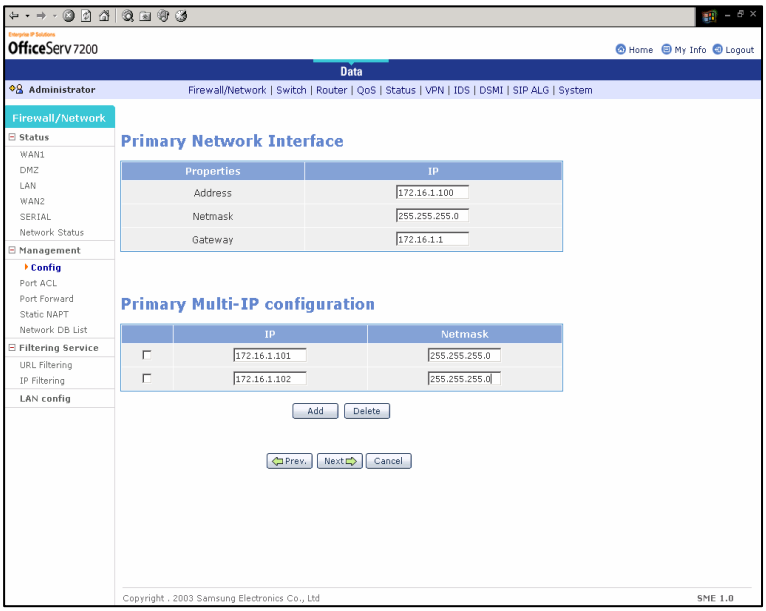
5.1. Static IP connection

If a static IP is used through Internet Service Provider, set to 'Fixed Line'. Click the [Next] button to move to the next step.



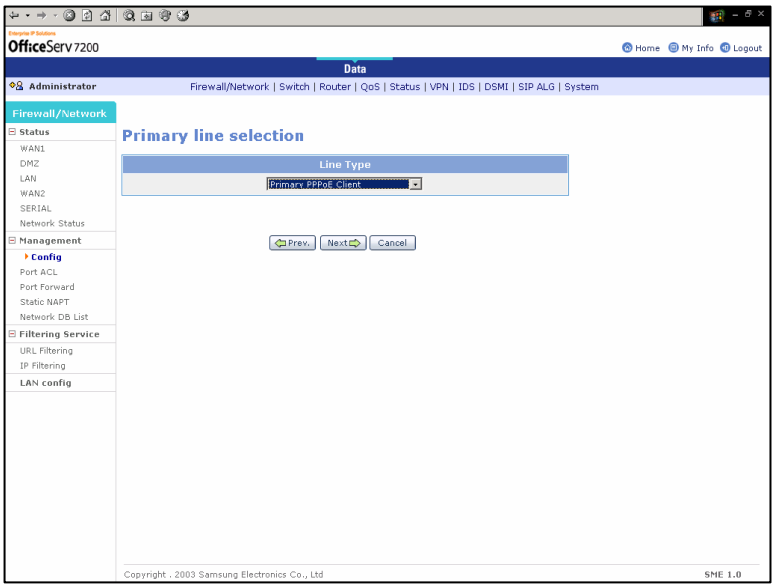
5.1.1. Set IP, Netmask, Gateway information on the WAN1 port. Check with your ISP for this information. Click the [Next] button to move to the next step.

5.1.2. If your Internet connection has multiple public IP addresses, under Primary Multi-IP configuration, click [Add] to add more public IP address.

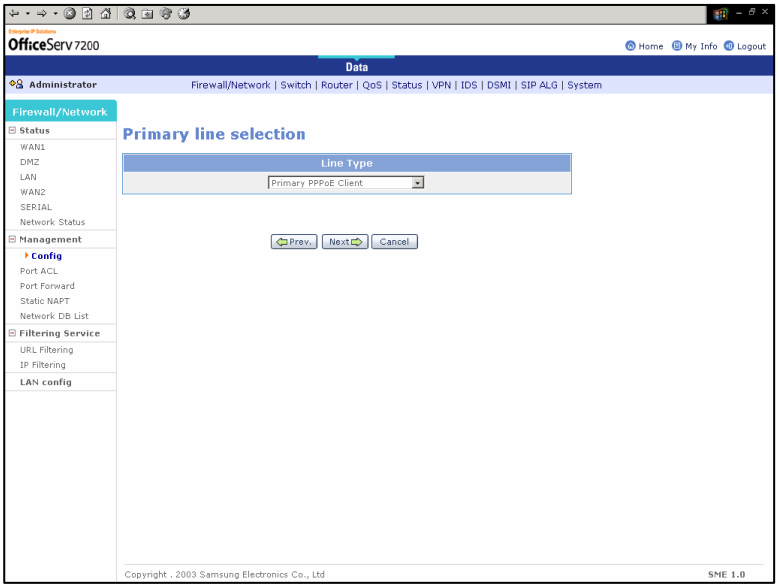


5.2. PPPoE (Point-to-Point Protocol over Ethernet)

If you use a DSL line and your DSL-based ISPs use PPPoE to establish Internet connections, set the WAN1 Primary Line Type to 'Primary PPPoE Client'. Click the [Next] button to move to the next step.



5.2.1. Enter your User ID and Password and click the [Next] button.



5.3. Obtain an IP Automatically

If your ISP automatically assigns an IP address, set the WAN1 Primary Line Type to 'Primary DHCP Client'. Click the [Next] button to move to the next step.

5.3.1. The line will be automatically configured. Click the [Next] button to move to the next step.

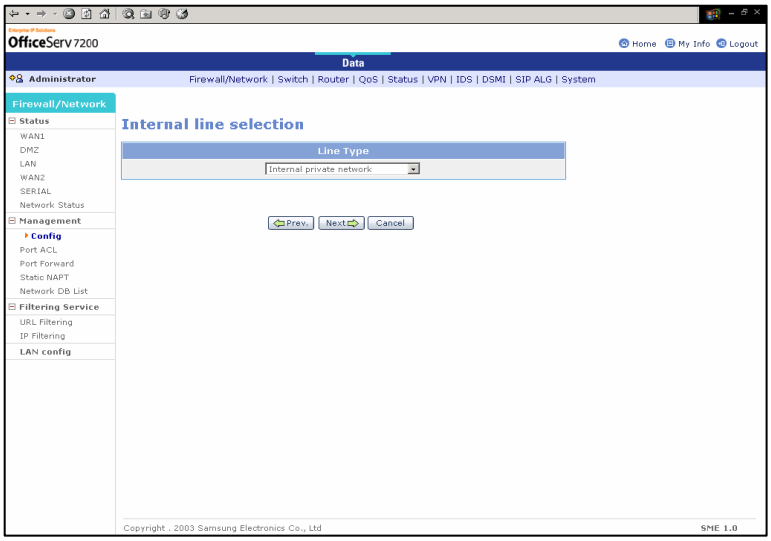
6. WAN1 ICMP Packet Reply settings determine if OS 7200 would respond to Ping command from external network. By default these settings are disabled.

7. WAN1 DDOS Prevention List settings enable the system to automatic detect and thwart Denial of Service attacks using the listed hacking programs.

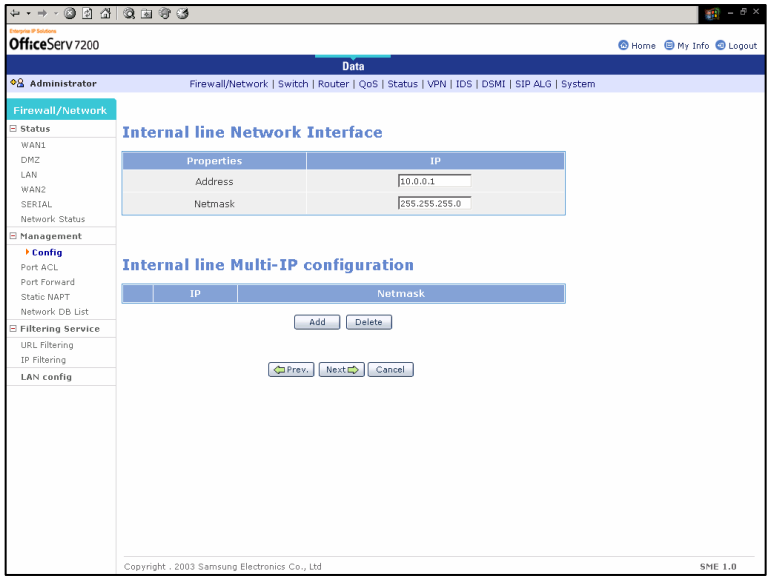
8. WAN1 DNS configuration sets the DNS address of the WAN1 port. Please check with your ISP for DNS server settings. Click the [Next] button to move to the next step.

© Samsung Telecommunications America, L.P.

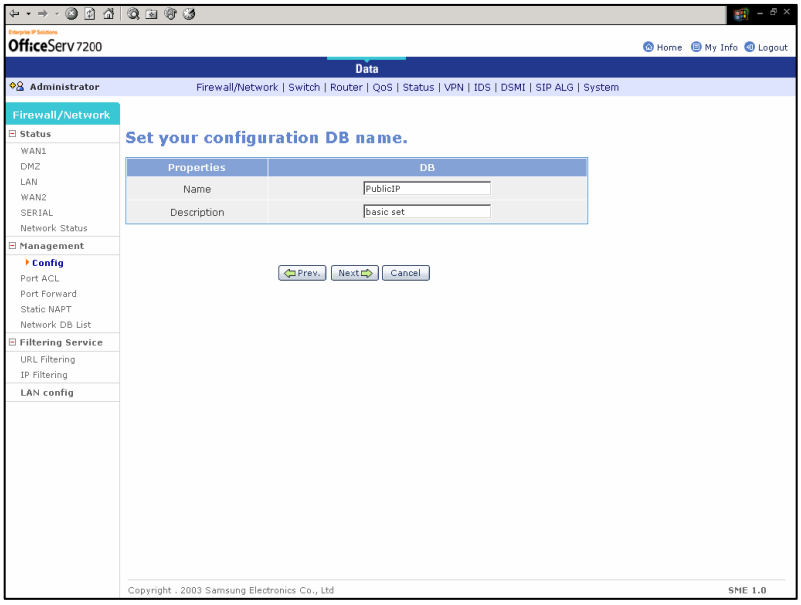
9. Set the LAN port line type set as 'Internal Line' to 'Internal private network'. Click the [Next] button to move to the next step.



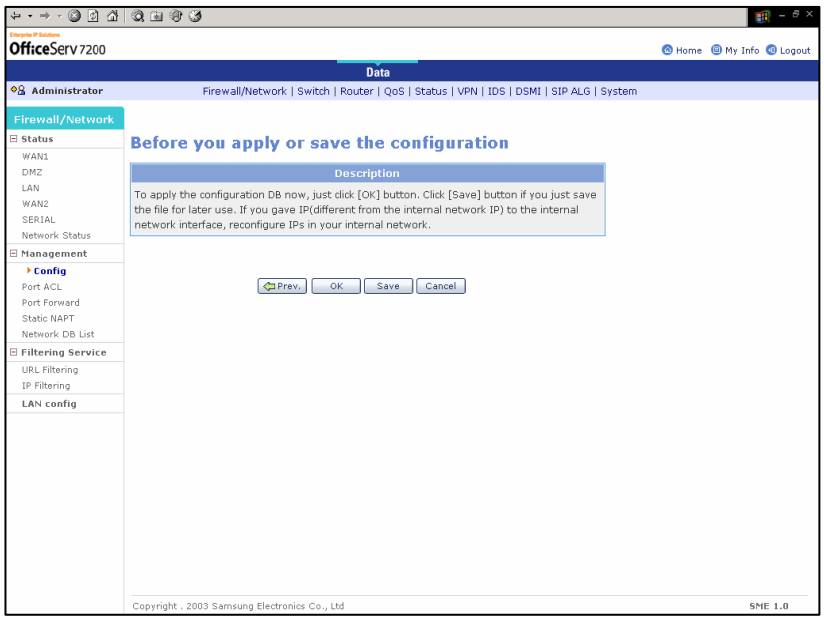
10. Set the LAN interface network. Enter 10.0.0.1 as IP. Click the [Next] button to move to the next step.



11. Save the settings(Steps 1-10) in database. Click the [Next] button to move to the next step.



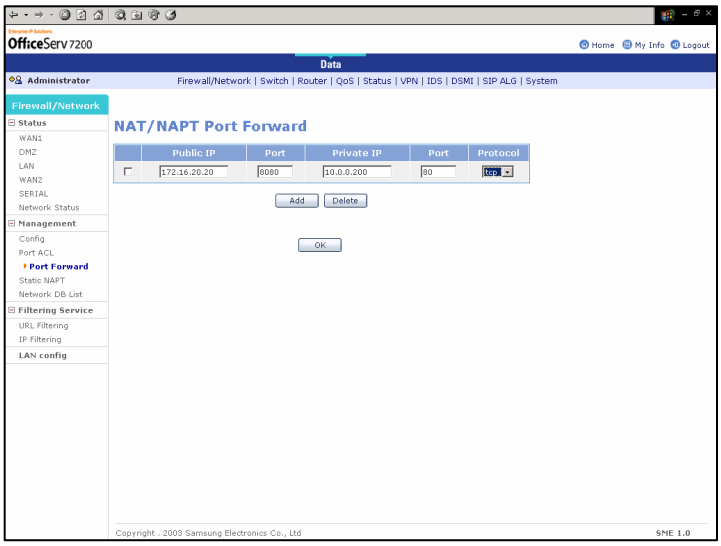
12. To apply the settings to the system, click the [Save] button, and click the [OK] button. If the [OK] button is not pressed, the settings are not applied to the system.



© Samsung Telecommunications America, L.P.

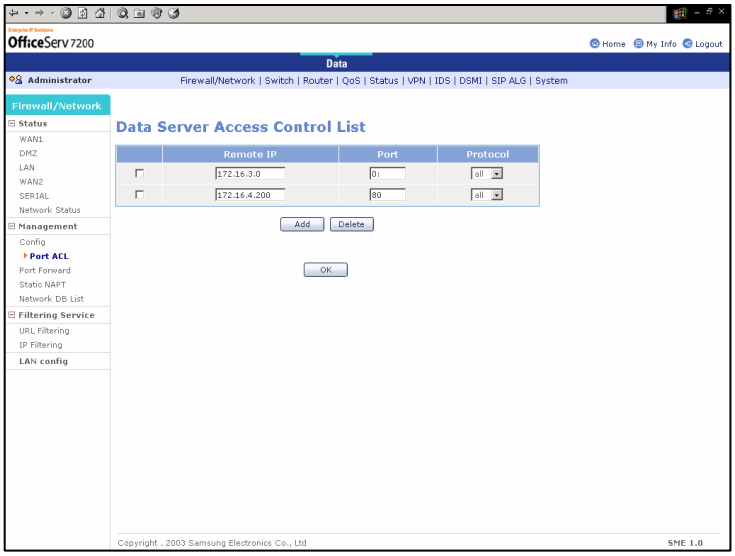
13. Configuring Port Forwarding

Go to [Firewall/Network] -> [Management] -> [Port Forward] to configure Port Forwarding. Although OfficeServ 7200 NAT router prevents Internet users from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request. If a range of port is required to be specified, use the 'Static NAPT' menu.



14. Configuring Port Access Control List

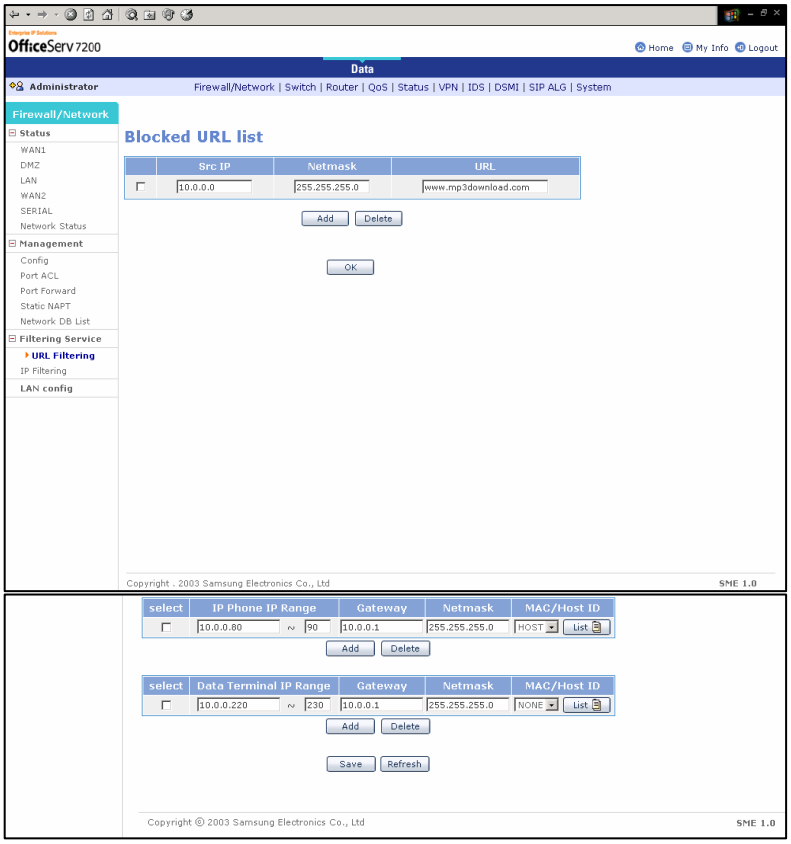
Go to [Firewall/Network] -> [Management] -> [Port ACL] to configure Port Access Control List. As the 'Packet Filtering' service is enabled, all external networks are restricted from accessing the Data Server. The Data Server Access Control List allows specific external servers or hosts to access the firewall based on port and protocol. If the port is set to '0:', the access to all ports is allowed. Click the [OK] button to move to the next step.



© Samsung Telecommunications America, L.P.

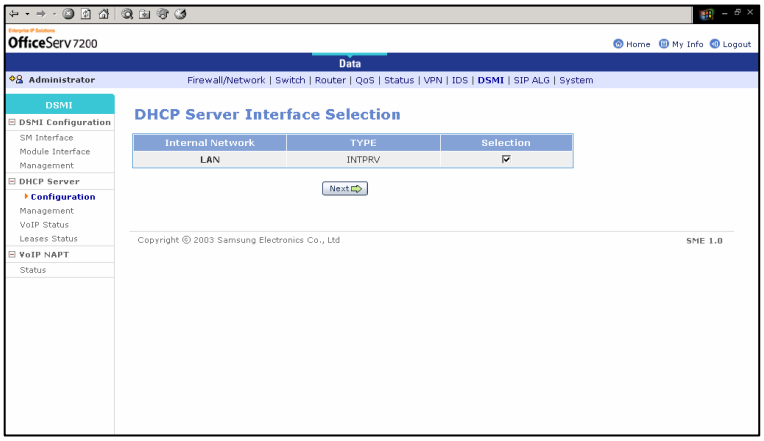
15. Configuring Packet Filtering

OS 7200 uses packet filtering to restrict the LAN network users from accessing the internet based on IP address and port and/or domain name and port. This can be configured under [Firewall/Network] → [Filtering Service] → [URL Filtering] and [IP filtering] menus.



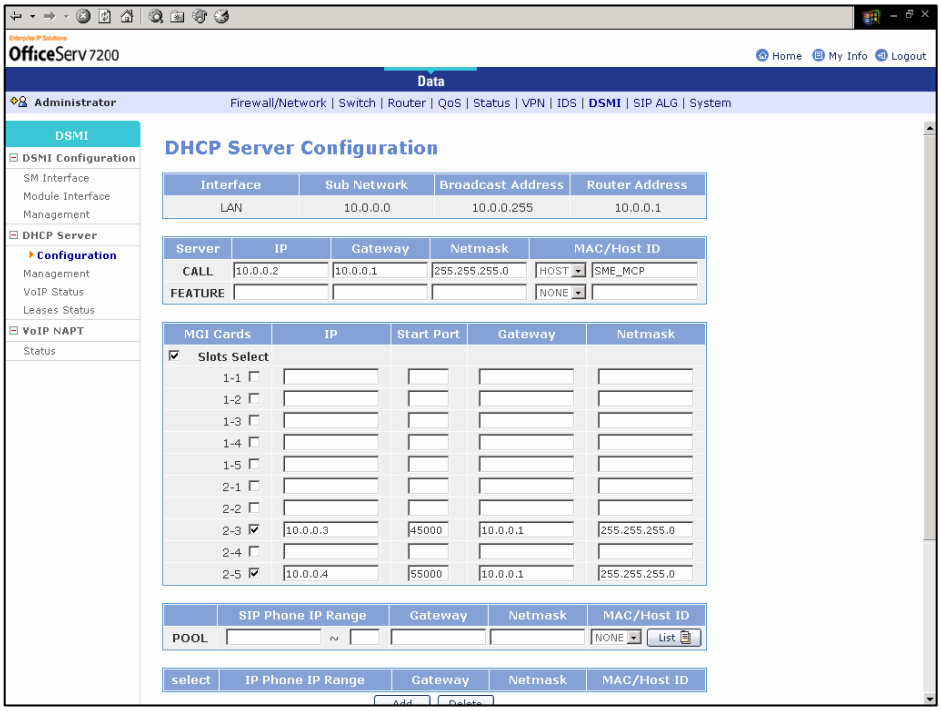
16. Configuring DHCP Server

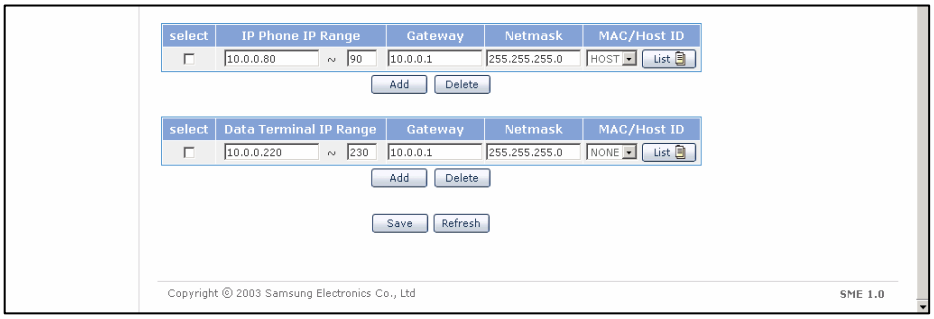
OS 7200 dynamically assigns network configuration information to attached PCs or network devices on the LAN using DHCP. By default, OS 7200 DHCP function is disabled. Go to [DSMI]-> [DHCP server] -> [Configuration] menu, select LAN 'Internal Network' and click the [Next] button to configure the DHCP server.



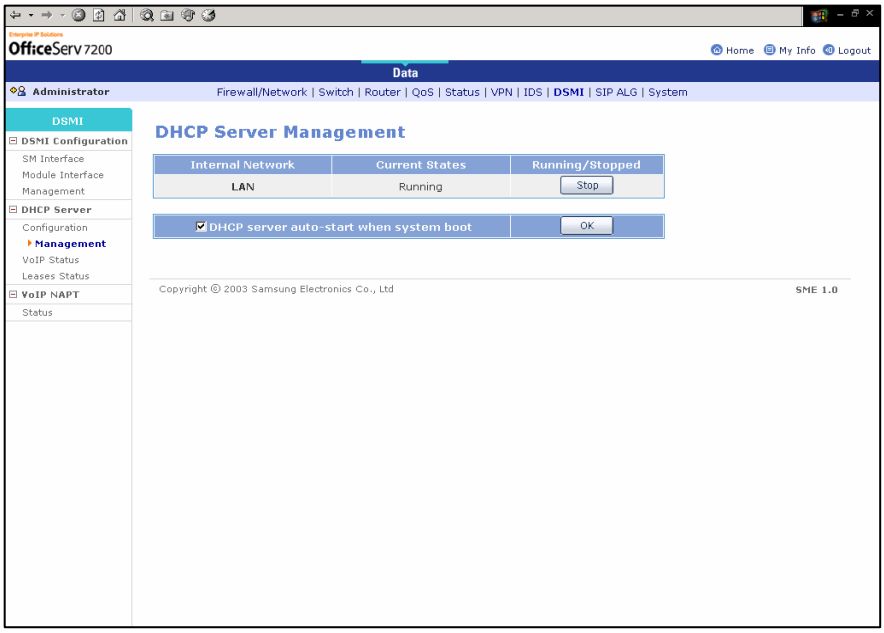
17. Create an IP Pool to be assigned from the DHCP service. The figure below shows that an IP Pool for a data terminal(PC) is created.

If you want to create an IP Pool to be assigned to ITP, set the range of an IP to be assigned to 'IP Phone IP Range'. If authentication method is set to 'HOST', the authentication is performed as the preset 'HOST ID'.

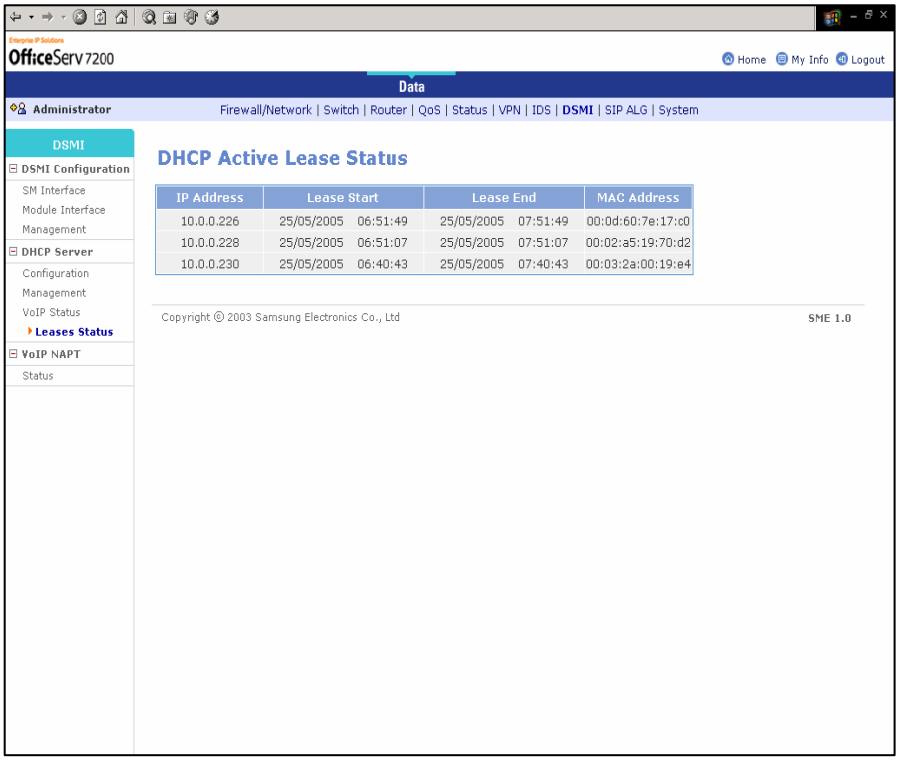




18. Go to [DSMI] -> [DHCP Server] -> [Management], press the [Run] button to execute the DHCP service. If the DHCP Server is required to automatically start when system reboots, check 'DHCP Server auto-start when system boot' and press the [OK] button.



19. You can check the DHCP client lease status by selecting [Lease Status] Menu.



OfficeServ 7200 Data Server Software Upgrade Quick Setup Guide

This Quick Setup Guide is designed to provide you with basic setup procedures of upgrading your OfficeServ 7200 Data Server software.

STEP 1: Install the WIM and LIM

1. Before you begin, power down the OfficeServ 7200 system. Insert WIM to Slot 1 and LIM to Slot 2 of the system (Basic or Expansion). In order to connect the WIM and LIM via the back panel of the system, the Jumpers on WIM module JP1 through JP4 should be set toward the back of the module as shown in the Figure 1-2 below.

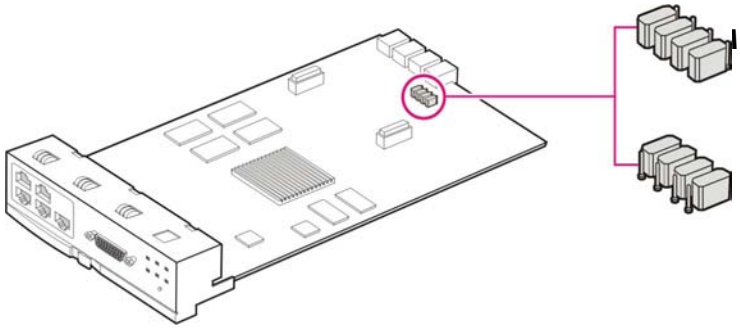


Figure 1-1
Connect the WIM module's LAN port to LIM on slot 2 using the Ethernet port of the front panel.

Figure 1-2
Connect with the LIM on slot 2 through the back panel.

Figure 1. Jumpers JP1 though JP4 on the WIM Module

2. Power on OS 7200. Connect one end of an Ethernet network cable to one of the LAN ports on the LIM module, and the other end to an Ethernet port on a PC.

STEP 2: Configure the PC

The LAN port on the WIM has the default IP address of 10.0.0.1/24. In order to connect to OS 7200 Data Web Management, configure your PC IP address to the same network. The following instructions apply only to Windows 2000 or XP.

1. Click the **Start** button, select **Settings** and click the **Control Panel** icon. Double-click the **Network and Dial-up** Connection icon.

2. Select the **Local Area Connection** for the applicable Ethernet adapter. Double-click the **Local Area Connection** and select the **Properties** button.

3. Highlight **Internet Protocol (TCP/IP)**, and select the **Properties** button.

© Samsung Telecommunications America, L.P.

4. Select **Use the following IP address**. Set the IP address to the following:

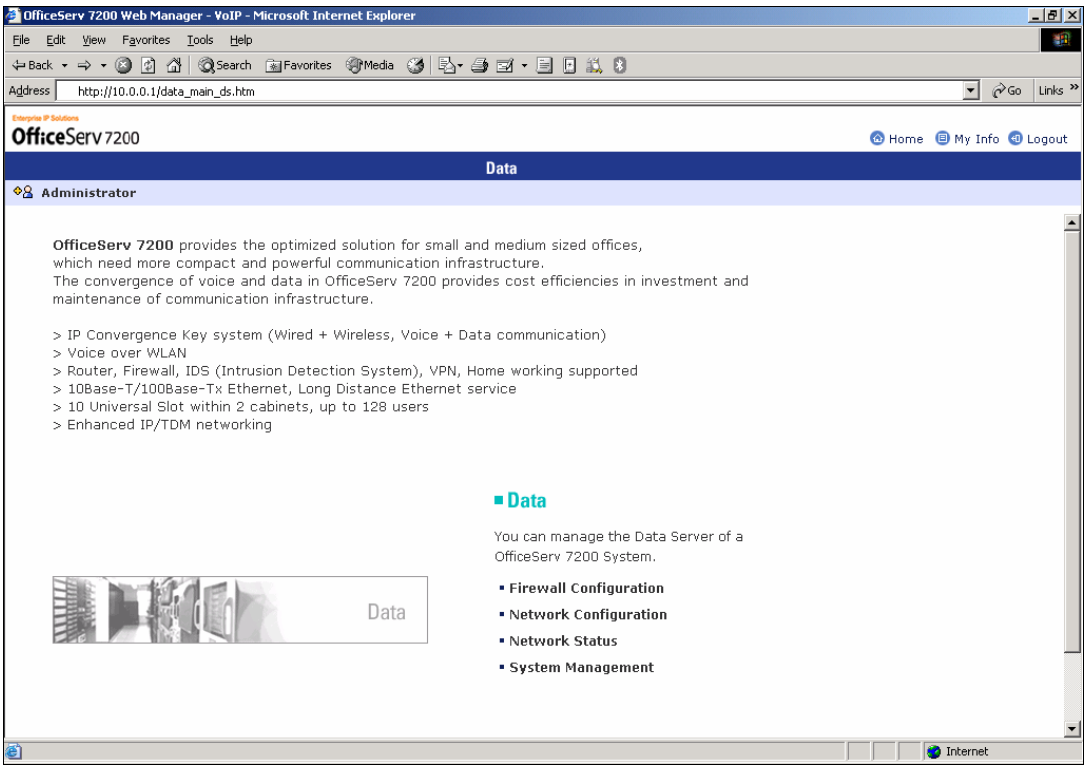
   IP Address: select from the range of 10.0.0.2 – 10.0.0.254
   Subnet Mask: 255.255.255.0
   Default Gateway: 10.0.0.1

5. Click the OK button to complete the PC configuration.

STEP 3: WIM Software Upgrade

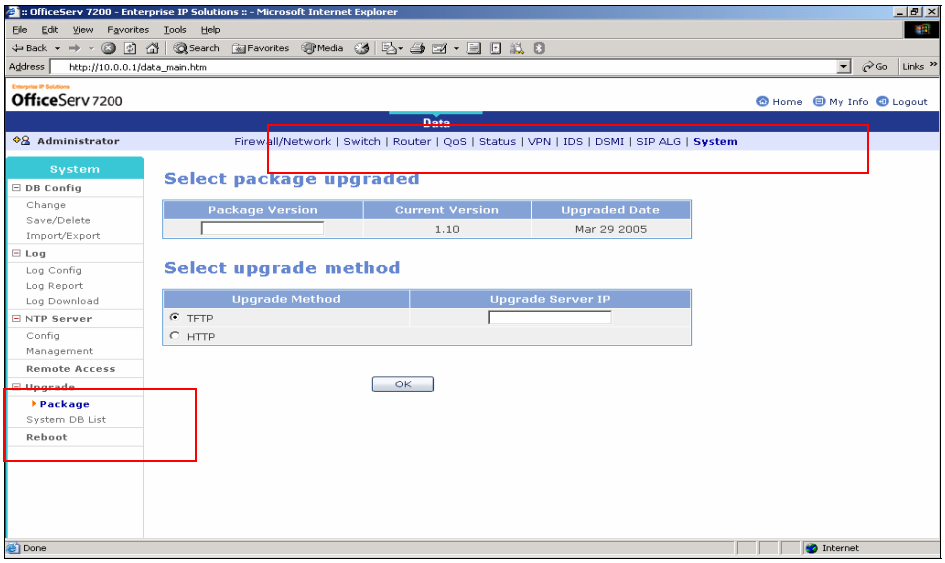
1. Open Microsoft Internet Explorer (version 6.0 or above) and enter the IP address of the LAN port on the WIM module in its Address field (The default is 10.0.0.1). Press the Enter key.

2. A password request screen will appear. Enter the default ID and Password, (the default ID and Password are **admin**, **admin** in the lowercase letters). Then click the **OK** button and following screen will appear:


OfficeServ 7200 Web Manager - VoIP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.0.0.1/data_main_ds.htm
OfficeServ 7200
Home My Info Logout
Data
Administrator
OfficeServ 7200 provides the optimized solution for small and medium sized offices, which need more compact and powerful communication infrastructure.
The convergence of voice and data in OfficeServ 7200 provides cost efficiencies in investment and maintenance of communication infrastructure.
> IP Convergence Key system (Wired + Wireless, Voice + Data communication)
> Voice over WLAN
> Router, Firewall, IDS (Intrusion Detection System), VPN, Home working supported
> 10Base-T/100Base-Tx Ethernet, Long Distance Ethernet service
> 10 Universal Slot within 2 cabinets, up to 128 users
> Enhanced IP/TDM networking
Data
You can manage the Data Server of a OfficeServ 7200 System.
Firewall Configuration
Network Configuration
Network Status
System Management
Data
Internet

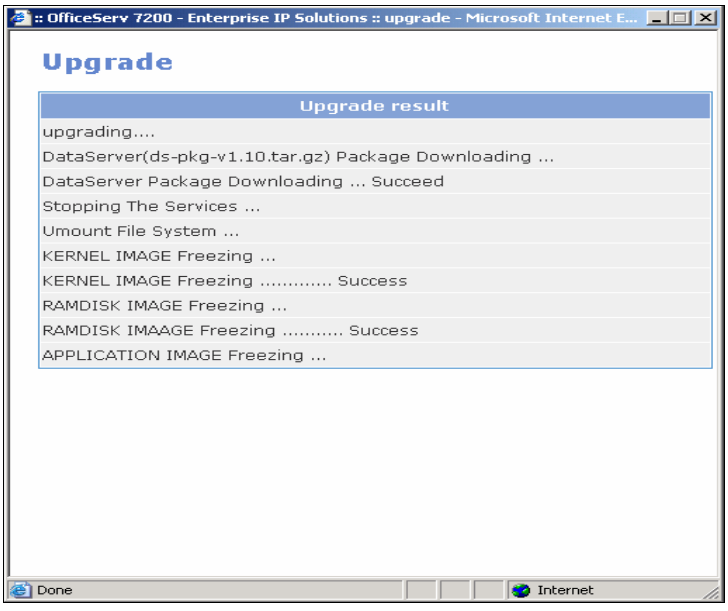
3. Click on **Data**, and select **System** on the top menu bar. Under System, the sub-menu will appear on the left hand side of the panel. Select **Upgrade** -> **Package,** as shown in the figure on the following page.

© Samsung Telecommunications America, L.P.



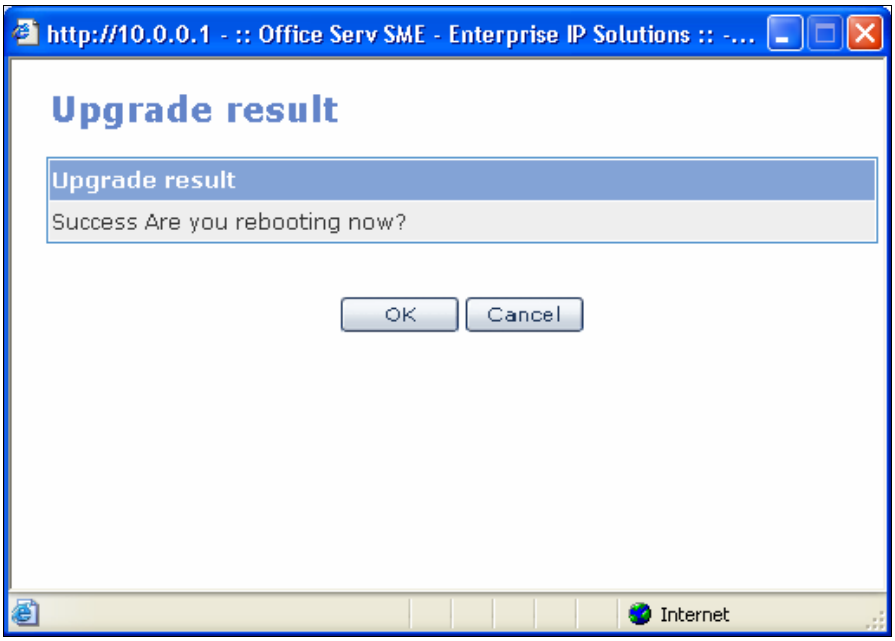
4. Under the **Select package upgraded**, enter the new WIM S/W package version X.XX in the **Package Version** field. Under the **Select upgrade method**, select the HTTP and click **OK**. If you are using Windows XP, please turn off the pop-ups blocker for the OS 7200 Data Web Management site (under Internet Explore Tools menu, select 'Always Allow Pop-ups from This Site…).

5. The **File upload** pop-up window appears. Click the **Browser** to search the upgrade file in the format of '**ds-pak-v{version_number}.tar.gz**'. Click **OK** to start the upgrade process as shown in the **Upgrade result** window below.



© Samsung Telecommunications America, L.P.

6. Once the upgrade process is completed and successful, click **OK** to reboot the system.



7. After the system is back in service, before log back into the Web Browser Data Server Management, please remember to clear the temporary cache in your Internet Explorer. Under Internet Explore, go to **Tools** -> **Internet Options**, and select **Delete Files** and **Delete Cookies**.

© Samsung Telecommunications America, L.P.

ABBREVIATION

A

ALG	Application Level Gateway
AH	Authentication Header
ARP	Address Resolution Protocol

C

CTI	Computer Telephony Integration

D

DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
DNS	Domain Name Server
DRR	Deficit Round Robin

E

ESP	Encapsulating Security Payload

H

HDLC	High-level Data Link Control

I

IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPSec	IP Security Protocol

L

LAN	Local Area Network

N

NAT	Network Address Translation
NMS	Network Management System

P

PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PVC	Permanent Virtual Circuit
PVID	Port VLAN Identification

S

STP	Spanning Tree Protocol
SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol

V

VLAN	Virtual Local Area Network